NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURITY AND EFFICIENCY CONCERNS WITH DISTRIBUTED COLLABORATIVE NETWORKING ENVIRONMENTS

by

Keith A. Felker

September 2003

Thesis Advisor:	Geoffrey Xie
Co-Advisor:	John Gibson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2003	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Security and Efficiency Concerns with Distributed Collaborative Networking Environments			**5. FUNDING NUMBERS**
6. AUTHOR(S) Keith A. Felker			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distributed is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The progression of technology is continuous and the technology that drives interpersonal communication is not an exception. Recent technology advancements in the areas of multicast, firewalls, encryption techniques, and bandwidth availability have made the next level of interpersonal communication possible.

This thesis answers why collaborative environments are important in today's online productivity. In doing so, it gives the reader a comprehensive background in distributed collaborative environments, answers how collaborative environments are employed in the Department of Defense and industry, details the effects network security has on multicast protocols, and compares collaborative solutions with a focus on security. The thesis ends by providing a recommendation for collaborative solutions to be utilized by NPS/DoD type networks. Efficient multicast collaboration, in the framework of security is a secondary focus of this research. As such, it takes security and firewall concerns into consideration while comparing and contrasting both multicast-based and non-multicast-based collaborative solutions.

14. SUBJECT TERMS Security and Efficiency Concerns with Distributed Collaborative Networking Environments, Collaborative Environments in the Department of Defense and Industry, Effects of Network Security on Multicasting, Collaborative Solutions, Collaboration, Multicast, Firewall			**15. NUMBER OF PAGES** 117
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SECURITY AND EFFICIENCY CONCERNS WITH DISTRIBUTED COLLABORATIVE NETWORKING ENVIRONMENTS

Keith A. Felker
Lieutenant, United States Navy
B.S., University of Illinois at Chicago, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2003

Author: Keith A. Felker

Approved by: Geoffrey Xie
Thesis Advisor

John Gibson
Co-Advisor

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The progression of technology is continuous and the technology that drives interpersonal communication is not the exception. Recent technology advancements in the areas of multicast, firewalls, encryption techniques, and bandwidth availability have made the next level of interpersonal communication possible.

This thesis answers why collaborative environments are important in today's online productivity. In doing so, it gives the reader a comprehensive background in distributed collaborative environments, answers how collaborative environments are employed in the Department of Defense and industry, details the effects network security has on multicast protocols, and compares collaborative solutions with a focus on security. The thesis ends by providing a recommendation for collaborative solutions to be utilized by NPS/DoD type networks. Efficient multicast collaboration, in the framework of security was a secondary focus of this research. As such, it takes security and firewall concerns into consideration while comparing and contrasting both multicast-based and non-multicast-based collaborative solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost I'd like to thank my wife Sierra for her support and understanding. She is my pillar and best friend. Additionally, I'd like to thank Dr. Xie and John Gibson, my thesis advisors, for their professional guidance and valuable insights. I would also like to thank Dr. Bordetsky, of the Naval Postgraduate School, for making the Groove Desktop environment available for my use. Finally, I'd like to thank Lonna Sherwin, Naval Postgraduate School network administrator, for taking time out of her busy schedule of wrestling with the latest viruses to discuss the schools network architecture.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The progression of technology is continuous and the technology that drives interpersonal communication is not an exception. The telegraph was a modern marvel in its time. Eventually it was replaced by the telephone. The advent of the facsimile machine, email, and instant messages expanded the functionality of the telephone and greatly contributed to the advance of interpersonal communication. Each of these communication advances has profoundly impacted society and how society conducts business. Recent technology advancements have made the next level of interpersonal communication possible.

This thesis answers why collaborative environments are important in today's online productivity. In doing so, it gives the reader a comprehensive background in collaborative environments, answers how collaborative environments are employed in the Department of Defense and industry, details the effects network security has on multicast protocols, and compares collaborative solutions with a focus on security. The thesis ends by providing a recommendation for collaborative solutions to be utilized by NPS/DoD type networks.

A. WHY COLLABORATIVE ENVIRONMENTS?

The ability to effectively collaborate in real-time over both local and wide area networks is the next step in the evolution of Internet services. Ray Ozzie, the CEO of Groove Networks, stated, "The next ten years will find us moving decidedly from an era of personal productivity and social software. That will involve a move from tightly coupled systems to more loosely coupled interconnections. It will be an era of highly interdependent systems and relationships, with technology continuing to reshape the nature of organizations, economy, society and personal lives." [2] Many other visionaries concur with Ozzie's prediction. We are at the brink of more coherent and compelling collaborative environments.

From an Internet perspective, collaborating via the Internet started with a tool that is approximately 30 years old, E-mail. A communication cornerstone, E-mail has become one of modern society's predominant methods of collaborating with others. However, E-mail has been quickly expanding to real-time collaboration environments, as provided by instant messaging.

In the near future, the computer will answer our phone calls; however, prior to answering the call the computer will prioritize the importance of the call and retrieve all of the caller's email, including background information. As the conversation commences, a screen sharing session will automatically be initiated allowing you to invite others to the conference, take notes, schedule events, etc.

B. BACKGROUND

The background section provides an overview of the basic concepts behind firewalls, multicasting, and cryptography. More specifically, the firewall section will discuss the types of firewalls that are commonly employed, the types of access mechanisms, and some examples firewall network configurations. In the area of multicasting, this section gives the reader a general understanding of IP multicasting, identifies key differences between hardware and Ethernet multicasting, and describes how mapping of multicast addresses to MAC addresses is done. It closes with a short section on cryptography that covers common terms and notations, throughout this thesis, as well as the main types of cryptography and their differences.

C. COLLABORATIVE ENVIRONMENTS IN THE DEPARTMENT OF DEFENSE AND INDUSTRY

This section further explains on why collaborative environments are being integrated into today's productivity solutions. The overall intent of this section is to solidify the reader's understanding of collaborative environments. In doing so, a general classification of collaboration and the collaborative process is briefly discussed. More

importantly, this section includes examples of collaborative environments that are currently employed in both industry and the Department of Defense.

D. EFFECTS OF NETWORK SECURITY ON MULTICASTING

This section addresses the role of multicast firewalls, tunneling, bandwidth management, multicast security differences, efficiency costs of authentication, and firewall specifics at NPS. More specifically, tunneling effects on efficiency are discussed and how multicast firewalls can be used in place of tunneling. Also, discussed is how packet replication can be optimized via the multicast group membership management. The section closes with multicast security differences, cost of authentication and firewall/multicast capabilities at the Naval Postgraduate School.

E. COMPARISON OF COLLABORATIVE SOLUTIONS WITH A FOCUS ON SECURITY

As many emerging technologies develop, a variety of implementation methods normally result. The mechanisms delivering the technology often result in a plethora of options for the end user. Although collaborative environments have been in existence for some time, the technology that delivers collaborative solutions is approaching new highs. Available collaboration solutions are abundant and can be found with numerous features serving the casual home user all the way to the largest of enterprises. Today's collaborative solutions provide services ranging in robustness, applicability, security, and ease of implementation. Collaborative technologies and solutions are in a continual development phase. Unfortunately, as with any new technology and/or solution, not only must the customer be wary, but also the developer. On one hand, the customer is faced with understanding the collaborative needs and/or requirements that best fit their organization. On the other hand, the collaborative developer is faced with understanding the needs of the customer and the limitations of the internet infra-structure and/or

developing standards. This understanding of needs coupled with unforgiving technology based industry, makes for an interesting topic of comparing collaborative solutions.

As a primary thesis focus, this section provides an in-depth comparison of collaborative solutions. More specifically, it points out the existence of numerous solutions then describes the various aspects that should be considered when selecting a collaborative solution (i.e. network architecture, security, and efficiency). The intent of this section is not to select best possible solution through an unrealistic exhaustive analysis of each available collaborative tool, but to impart upon the reader the areas of concentration that will assist in selecting the a collaborative tool that fits a particular organization.

F. INTRODUCTION SUMMARY

Understanding why collaborative environments are important in today's online productivity is the first step in selecting a collaborative solution. A comprehensive background in collaborative environments coupled with knowing what collaborative solutions are available will greatly assist in deciding which collaborative solution 'best fits' an organization. Finally, understanding the impact of network security on collaborative environments will help to ascertain the appropriate level of security for a desired level of collaborative robustness.

II. BACKGROUND

This section provides an overview of the basic concepts behind firewalls, multicasting, and cryptography. More specifically, the firewall section will discuss the types of firewalls that are commonly employed, the types of access mechanisms, and some examples firewall network configurations. In the area of multicasting, this section gives the reader a general understanding of IP multicasting, identifies key differences between hardware and Ethernet multicasting, and describes how mapping of multicast addresses to MAC addresses is done. It closes with a short section on cryptography that covers common terms and notations, throughout this thesis, as well as the main types of cryptography and their differences.

A. FIREWALLS

A firewall is simply a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. They are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All data entering or leaving the Intranet pass through the firewall, which examines each packet and blocks those that do not meet the employed security criteria. Generally, firewalls are configured to protect against unauthenticated interactive logins from the outside world. This helps prevent "hackers" from logging into machines on the protected network. More sophisticated firewalls block traffic from the outside to the inside, but permit users on the inside to communicate a little more freely with the outside. Firewalls are essential, since they can provide an important logging and auditing function, at a single check point, which may provide summaries to the administrator about what type and volume of traffic has been channeled through it. This is an important point: providing this check point can serve an analogous purpose for the network resources as an armed guard for the physical premises. [5]

1. Types of Firewalls

Theoretically, there are two types of firewalls: network layer, and application layer. [5] The difference between these firewalls is subtle. It centers on what mechanisms the firewall uses to examine and filter traffic from one security zone to another. The International Standards Organization (ISO) Open Systems Interconnect (OSI) model for networking defines seven layers, where each layer provides services that higher-level layers depend on. The important thing to recognize is that the lower the implementation level of the forwarding mechanism, the less examination of the encapsulated data the firewall can perform.

a. Network Layer Firewalls

This type of firewall generally makes its decisions based on the source address, destination address, and ports in individual IP packets. A simple router is the traditional network layer firewall. It is not able to make particularly complicated decisions regarding what resource a packet is communicating with or from where the packet came. Modern network layer firewalls, however, have become increasingly more sophisticated, and now maintain internal information about the state of connections passing through them at any time. One important difference about many network layer firewalls is that they route traffic directly though them, requiring a validly assigned IP address block or a private internet address block. The network layer firewalls tend to be very fast and mostly transparent to its users. [5]

b. Application Layer Firewalls

These generally are hosts running proxy servers, which permit no direct Layer 3 traffic between networks, and which perform elaborate logging and examination of traffic passing through them. Since proxy applications are simply software running on the firewall, it is a good place to perform extensive logging and access control.

Application layer firewalls can be used as network address translators, since traffic goes in one side and out the other, after having passed through an application that effectively masks the origin of the initiating connection. [5]

Having an application "in the middle" may impact performance and make the firewall less transparent. Early application layer firewalls were not particularly transparent to end-users and, if still employed, may require some training. However, more modern application layer firewalls are often totally transparent. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls. [5]

2. Functions and Methods of Firewall Operations

Firewalls function as access control mechanisms and normally reside at the gateway between two network nodes. Firewalls provide distinct advantages but also have some disadvantages. The advantages provided by firewalls, as access control mechanisms, are necessary for a network to function with a comfortable amount of security. Firewalls serve to support and enforce a network access control policy where in many cases the administrator is able to develop policies that state what data and services external users can and cannot access. Additionally, firewalls can perform logging of connections and network statistics, prevent IP Spoofing by outsiders, and block suspected attacks. Unfortunately, disadvantages of using firewalls exist. Since firewalls are concentrated in one place, firewalls can seriously impact bandwidth efficiency by creating bottlenecks for transiting data packets. Also, a break in a firewall can be catastrophic due to a single point of failure. Finally, firewalls don't address insider attacks.

The level of protection and security a firewall provides ranges from the single personal computer, to a small network, and even to the largest of enterprises. Firewalls can be setup in a variety of ways. Depending on an individual or organizations' needs, the setup can be a very simple or an extremely complex process. A more complicated setup is associated with greater protection and security. The access control mechanisms

employed by the firewall will dictate the degree of complexity of the setup and maintenance process. Regardless of a networks complexity, the mechanisms firewalls employ will consist of static packet filtering, dynamic packet filtering, and/or application gateways. [7]

a. Static Packet Filters

Static packet filters are the simplest of the firewall mechanisms. They are very fast and provide the best bandwidth efficiency. The transiting packets are rejected or allowed based upon packet header information. Source and destination IP addresses and port numbers, protocols, TCP flags are contained in the packet header information. Filtering source IP numbers allows the administrator to block traffic from suspected hosts. While filtering on the destination IP numbers allows specific types of traffic to be directed to specific internal systems. The destination port number and protocol completely specifies well known services such as: TCP port 25 being mail (STMP), TCP port 513 accesses the UNIX login functionality, UDP port 513 is the UNIX "who" command, HTTP port 80 is the web, and many others. Static packet filtering rules guard against IP spoofing, among other forms of malicious attacks.

b. Dynamic Packet Filters

Dynamic packet filtering has the advantages of static packet filtering but eliminates the 'block all' or 'allow all' aspect of static packet filtering. With dynamic filtering, packet header information is stored for future screening in a state information table. Prior to making a decision to drop or allow a packet, the new packet coupled, with the state information table, is checked against the relevant rule. This technique is particularly useful when screening UDP packets. In this case, the state information table will keep track of outgoing UDP requests and when a corresponding inbound UDP packet is received it will be allowed to pass through the firewall.

c. Application Gateways

Application Gateways generally consist of a number of application specific programs, called proxy servers. These proxy servers control access at the application layer. There are many different types of proxy servers. Proxy Servers can access web pages for other computers (increasing network efficiency by caching frequently visited web sites into its memory), establish sessions with other computers, and protect networked or home computers from malicious intent. For example, a File Transfer Protocol (FTP) proxy server will accept all incoming FTP traffic and establish a proxy session between the requester and the FTP server. In this case, the outside world will only know the IP address of the proxy server, not the FTP server. In addition, the FTP proxy server can mediate all FTP commands, increasing the security associated with the session. Hence, proxy servers can allow, or not allow, various protocol commands making it more difficult for hackers, anonymous or not, to implement their malicious actions.

3. Network Firewall Topologies

The following firewall network examples contain physical computers that function as dedicated firewalls. There are many firewall network configurations to choose from and the examples below are included for display purposes only.

a. Simple Dual-Homed Firewall

The dual-homed firewall (Figure 1 below) is one of the simplest implementations and is possibly the most common way to use a firewall. The Internet comes into the firewall directly via a dial-up modem or through some other type of external connection, like an ISDN line or cable modem. With this configuration, a demilitarized zone (DMZ) is not possible. [6] A DMZ is a portion of a network that is

normally outside the boundaries of the network's firewall (i.e. the area between a network and the Internet).

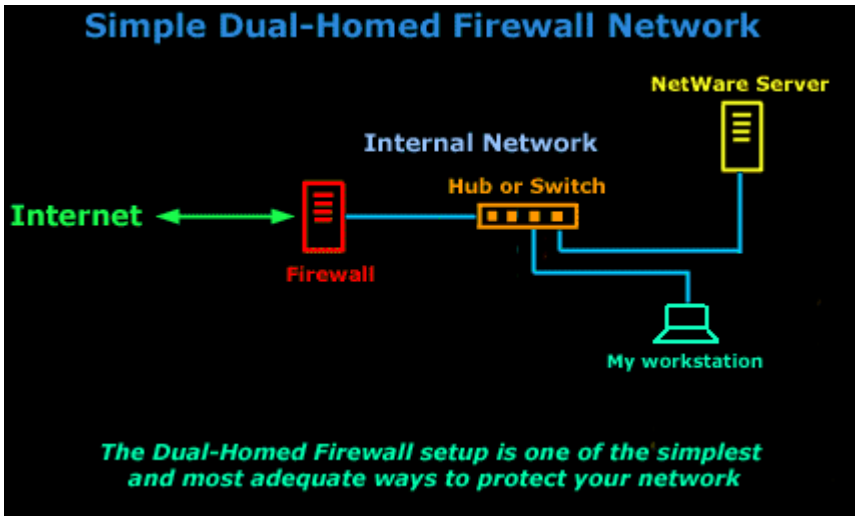


Figure 1. Simple Dual-Homed Firewall Network (from [6])

The firewall takes care of forwarding packets that pass its filtering rules between the internal network and the Internet, and vice versa. [6] This dual-homed host configuration can also function as IP masquerading. The two "homes" refer to the two networks that the firewall machine is part of - one interface connected to the outside home, and the other connected to the inside home. [6]

This particular setup has the advantage of simplicity. If the network's Internet connection is via the firewall's modem and contains only one IP address, then this simple network is the only option until a more complex network is created. [6]

b. Two-Legged Network with a Fully Exposed DMZ

This more advanced network configuration contains a router that connects a public server network located in the DMZ. This public network is located outside of the firewall and is isolated from the internal network. The internal network is connected by an internal hub (or switch), as shown in Figure 2.

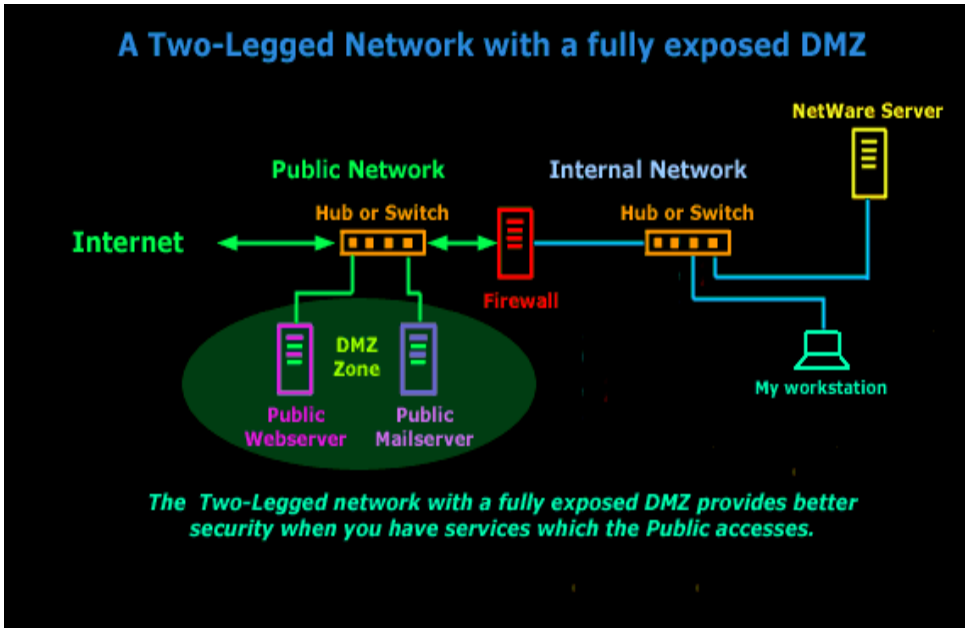


Figure 2. Two-Legged Network with exposed DMZ (from [6])

Machines that want direct access to the outside world, unfiltered by the firewall, connect to the external hub. One of the firewall's network adapters also connects to this hub. The other network adapter connects to the internal hub. Machines that need to be protected by the firewall need to connect to this hub. Any of these hubs could be replaced with switches for added security and speed, and it would be more effective to use a switch for the internal hub. Like the simple dual homed firewall, an advantage of the two legged network with an exposed DMZ configuration is that the firewall needs only two network cards. This simplifies the configuration of the firewall. Additionally, the router (located upstream between the Internet and the DMZ hub/switch) allows access to a second set of packet-filtering capabilities. Using these, gives a DMZ some limited protection while completely separate from the firewall. However, if the router is not controllable (i.e. administered by another entity), the DMZ is totally exposed to the Internet. Hardening a machine enough to live in the DMZ without getting regularly compromised can be tricky. [6] At minimum, a software based firewall should be implemented on any machine operating in the DMZ. The exposed DMZ configuration

depends on two things: 1) an external router located upstream between the Internet and the DMZ hub/switch, and 2) multiple IP addresses.

An alternate solution is required if any of the following conditions hold: 1) a modem link using PPP (modem dial-up), 2) the external router is administered by another party, 3) the configuration requires masquerading the DMZ, or 4) the network has only one IP address. There are two straightforward solutions. Depending on an organization's needs, the first solution is to build a second router/firewall, as depicted in Figure 3. This is useful if connecting via PPP. One machine acts as the exterior router/ firewall (Firewall No.1). This machine is responsible for creating the PPP connection and controls the access to the DMZ zone. The other firewall (Firewall No.2) is a standard dual-homed host and functions to protect the internal network. This is identical to the situation of a dual homed firewall where the PPP machine is the local exterior router.

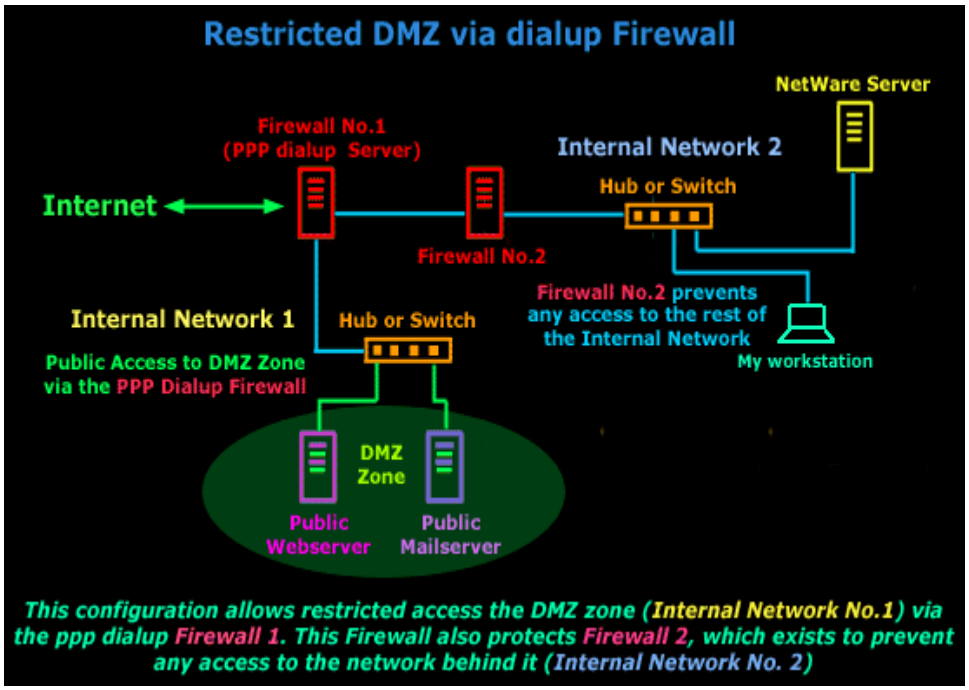


Figure 3. Restricted DMZ via dialup Firewall (from [6])

The second solution is to create a three-legged firewall, as described in the next section.

c. The Three-legged Firewall

In this configuration, an additional network adapter in the firewall host provides the external interface to the Internet, while isolating the public server farm from the internal network with the other two network interface adapters. The firewall is then configured to route packets between the outside world and the DMZ differently than between the outside world and the internal network. [6]

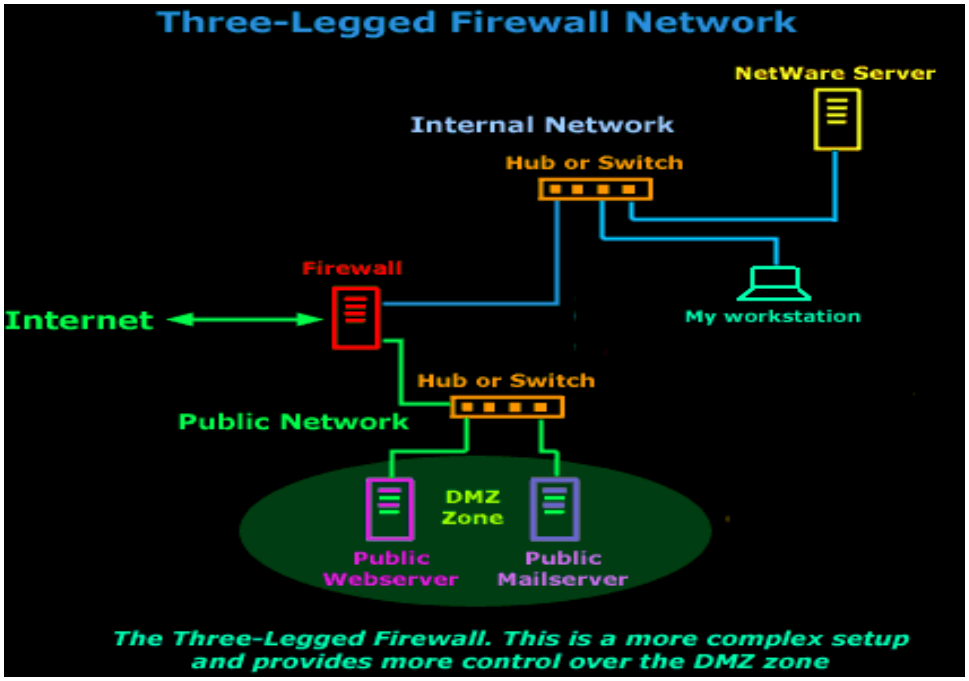


Figure 4. Three-Legged Firewall Network (from [6])

The three-legged setup can also give the ability to have a DMZ, as shown in Figure 4. Replace the external router (located between the firewall and the Internet) with a modem and the network is similar to the simple dual homed firewall topology with the inclusion of a segmented server farm. [6] If a network requires IP masquerading, the DMZ can do so while keeping the impacted hosts functionally separate from the protected internal machines. Network configurations that include cable modems or static PPP connections can use this system to run various servers within a DMZ as well as an

entire internal network off a single IP address. It's a very economic solution for small businesses or home offices. [6]

The primary disadvantage to the three-legged firewall is the additional complexity. Access to and from the DMZ and to and from the internal network is controlled by one large set of rules. [6]

4. Static vs. Dynamic vs. Application Filters

Static packet filters are very fast and cheap; however, their rule sets potentially could become very complicated and hard to test. Additionally, static packet filters do not support UDP query/response services well, or hide internal IP addresses. With static packet filters, a service must be either allowed or blocked. Conversely, dynamic filters have all the advantages of static filters without the course level of granularity. That is, they can support query/response type services and prevent port scans. Unfortunately, they are more costly than static packet filters. The application filters contain proxy servers that are application specific. The majority of commercial-off-the-shelf (COTS) firewalls come with a common set of proxies. If a special proxy is required, then the proxy must be written in-house or a custom proxy contracted for development. Application filters effectively hide internal IP addresses and filter at the application level. Unfortunately, these filters are the most expensive of firewall control mechanisms and can severely impact network performance. [7]

5. Firewall Summary

Future firewalls typically should incorporate features from both network layered firewalls and application layered firewalls. It is likely that network layer firewalls will become increasingly aware of the information going through them, and application layer firewalls will become more and more transparent. The end result will be kind of a fast packet-screening system that logs and checks data as it passes through the firewall. [5]

B. MULTICAST

Multicast is similar to a broadcast in the sense that its target is potentially more than one of the machines on a network. Where a broadcast is directed to all hosts on the network, a multicast is directed to a specific group of hosts. The network hosts can choose whether or not they wish to participate in the multicast group, whereas in a broadcast, all hosts are required to process the data unit, whether they want it or not. [3] Multicast group management is typically done with the Internet Group Management Protocol. A typical multicast on an Ethernet network, using the TCP/IP protocol, consists of two parts, Hardware/Ethernet multicast and IP Multicast, shown in Figure 5. [3]

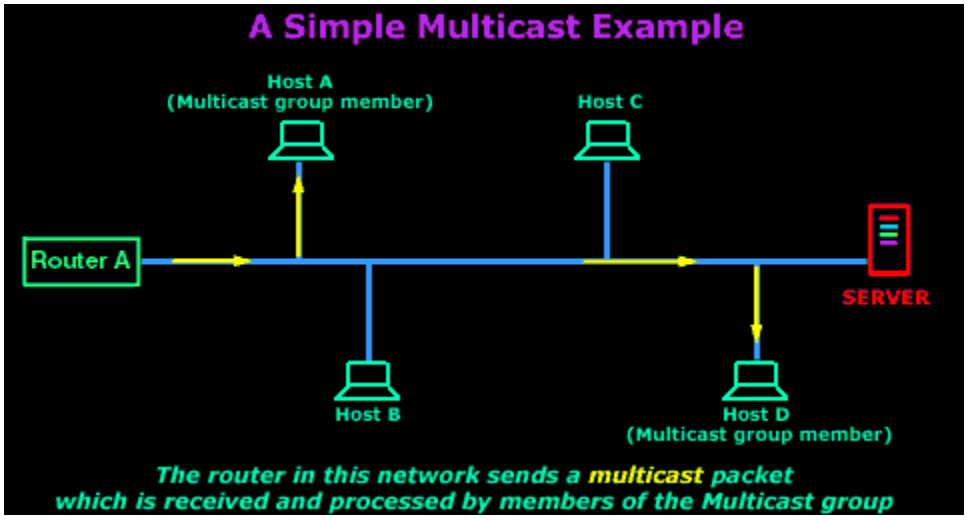


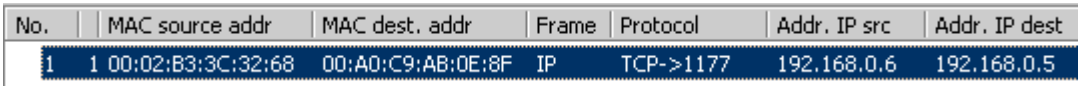
Figure 5. Simple Multicast Example (from [3])

1. Hardware/Ethernet Multicasting

When a computer joins a multicast group, it needs to be able to distinguish between normal unicast and multicast traffic. With hardware multicasting, the network card is configured, via its drivers, to watch for the particular multicast MAC addresses of the groups to which it belongs. When the network card receives a packet that contains a destination MAC address that matches any of the multicast MAC addresses for which it

is configured, it will pass the packet to the network layer for further processing. [3] This process is accomplished by the Ethernet using a low-order bit of the high-order octet to distinguish conventional unicast addresses from multicast addresses. A unicast would have this bit set to ZERO (0), whereas a multicast would be set to ONE (1). [3] Following is an example of each class of MAC address.

When a unicast packet is placed on the network by a computer, it contains the source and destination MAC addresses, as specified in the 2nd Layer of the OSI model. Figure 6 provides an example of information extracted from the Ethernet header of a unicast packet being sent to the network's gateway (192.168.0.5) by one of the workstations (192.168.0.6). Note that the figure also includes the layer 3 source and destination addresses, in this example IPv4 addresses. The least significant bit of the most significant byte (00) of the destination address is zero.



No.	MAC source addr	MAC dest. addr	Frame	Protocol	Addr. IP src	Addr. IP dest
1	1 00:02:B3:3C:32:68	00:A0:C9:AB:0E:8F	IP	TCP->1177	192.168.0.6	192.168.0.5

Figure 6. Sniffed Unicast Packet (from [3])

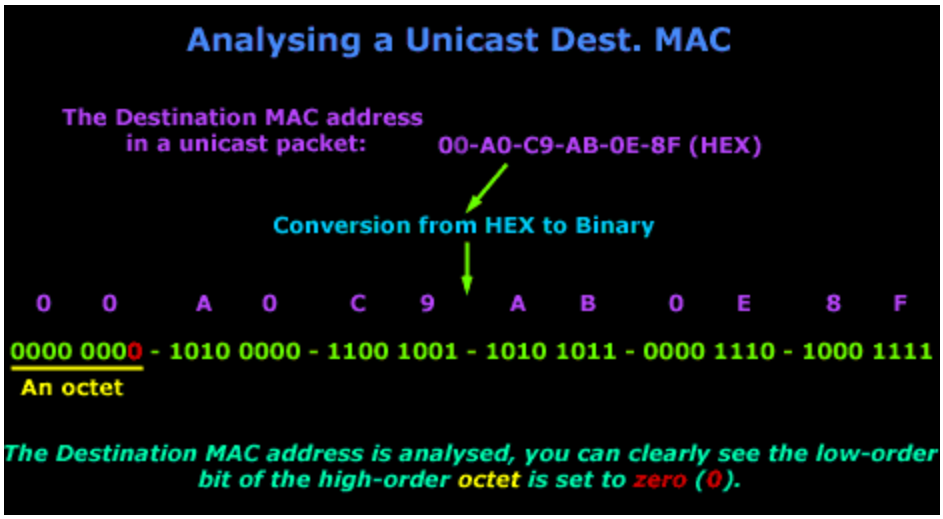


Figure 7. Analyzing a Unicast Destination MAC Address (from [3])

In a multicast packet, the packet will not be directed to one host but a group of hosts, so the destination MAC address will not match the unique MAC address of any

computer. However, the computers that are part of the multicast group will recognize the destination MAC address and accept it for processing. The multicast packet, whose header information is shown in Figure 8, was sent from a NetWare server. Notice the least significant bit of the most significant byte (01) of the destination MAC address is one, indicating that the destination is a multicast group.

No.	MAC source addr	MAC dest. addr	Frame	Protocol	Addr. IP src	Addr. IP dest
1	1 00:80:C8:F9:76:EF	01:00:5E:00:00:05	IP	OSPFIGP	192.168.0.2	224.0.0.5

Figure 8. Sniffed Multicast Packet (from [3])

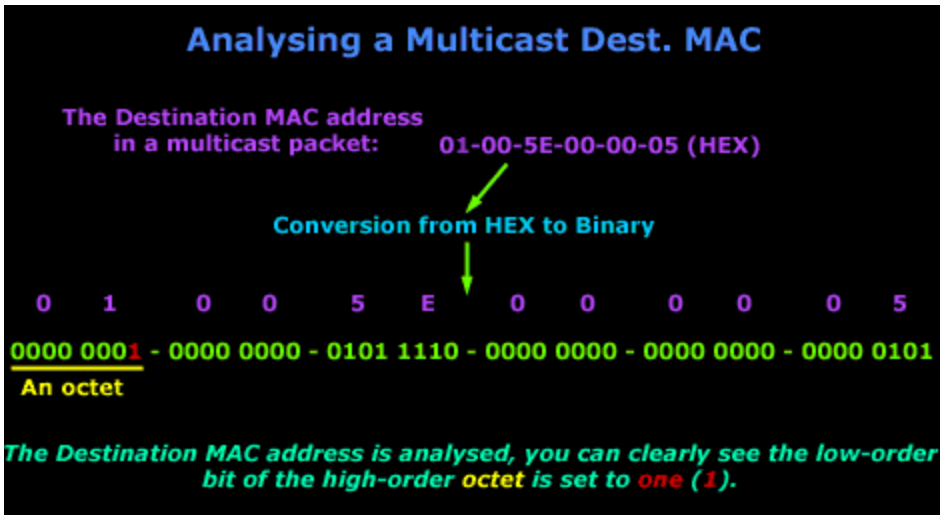


Figure 9. Analyzing a Multicast Destination MAC address (from [3])

Here, the destination MAC address, 01-00-5E-00-00-05, is not the address of a particular host-computer but, rather, the MAC address that can be recognized by computers that are part of the particular multicast group. The "particular" multicast group identified by the MAC address is actually a set of multicast groups, as explained in a later section. The source address is always a unicast address to identify the computer from which the packet came. [3]

2. IP Multicasting

In IP Multicasting, the hardware multicasting MAC address is mapped to an IP address. Once the Datalink Layer, layer 2, receives the multicast packet from the network, it will remove the MAC addresses and send the rest to the Network Layer. The Network Layer must be able to recognize the packet as being addresses to a multicast group, so the IP address is set in way that allows the computer to see it as a multicast datagram. Note that a host may send multicast datagrams to a multicast group without being a member. Multicasts are used frequently between routers so that they can discover each other across an IP network. For example, an Open Shortest Path First (OSPF) router sends a "hello" packet to other OSPF routers on the network. The OSPF router must send this "hello" packet to an assigned multicast address, specifically, group address 224.0.0.5. The other routers will respond will respond to this address. IP Multicast uses Class D IP Addresses:

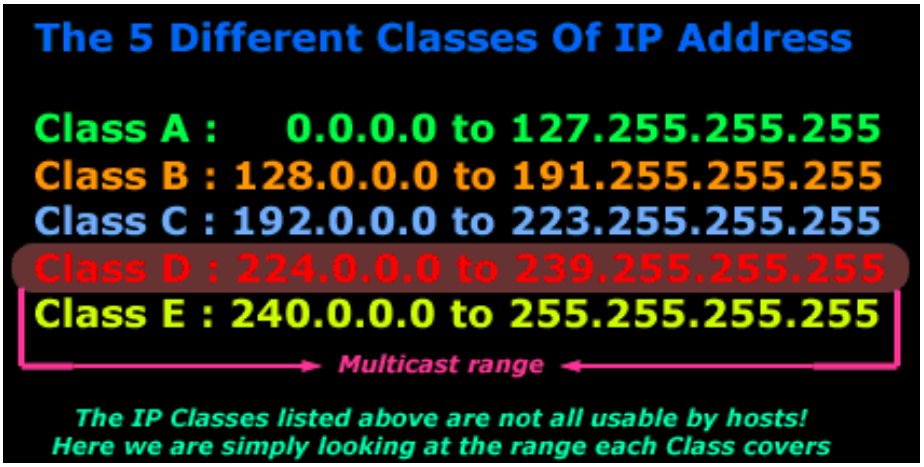


Figure 10. The 5 Different Classes of IP Address (from [3])

Figure 10 displays the different classes of IP address. The following list contains some examples of IP multicast addresses:

- 224.0.0.0 Base Address (Reserved) [RFC1112,JBP]
- 224.0.0.1 All Systems on this Subnet [RFC1112,JBP]
- 224.0.0.2 All Routers on this Subnet [JBP]

- 224.0.0.3 Unassigned [JBP]
- 224.0.0.4 DVMRP Routers [RFC1075,JBP]
- 224.0.0.5 OSPFIGP OSPFIGP All Routers [RFC2328,JXM1]

3. Mapping IP Multicast to Ethernet Multicast

To map an IP multicast address to the corresponding hardware/Ethernet multicast address, place the low-order 23 bits of the IP multicast address into the low-order 23 bits of the special Ethernet multicast address. The rest of the high-order bits are defined by the IEEE. This mapping process determines the hardware MAC address. Let's have a look at a real example to understand this. [3]

Using Multicast IP address 224.0.0.5, identified above as the multicast address for the OSPF routing protocol, as an example, Figure 11 presents the analysis of the IP address in binary format so the value of each bit can be seen.

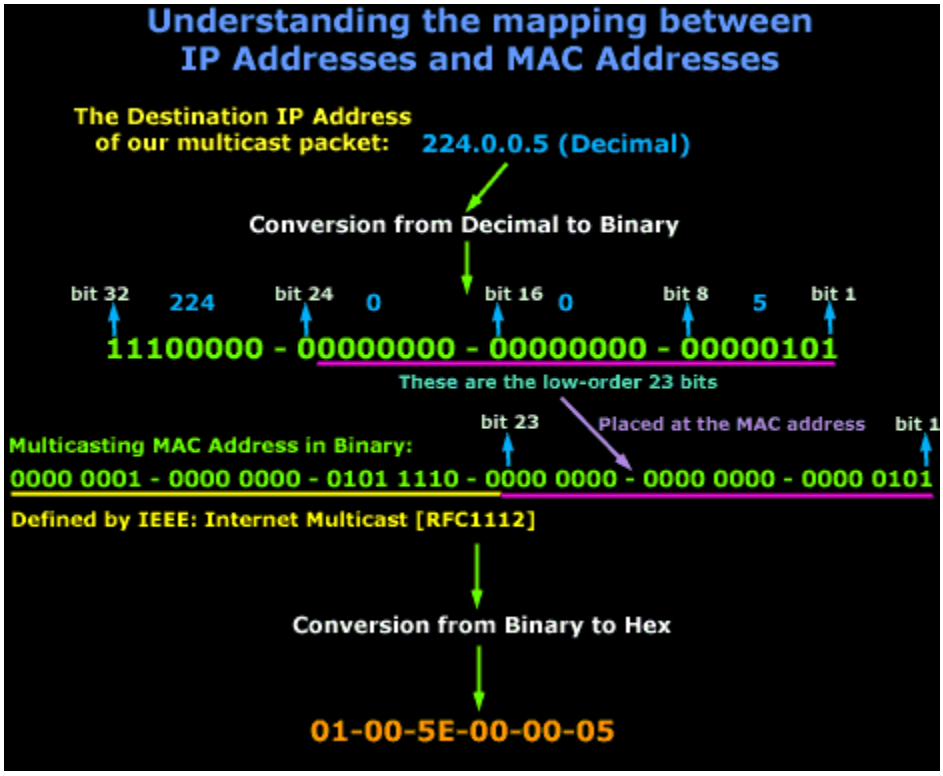


Figure 11. Mapping Between IP Addresses and MAC Addresses (from [3])

Multicast routers should not forward any multicast datagram with destination addresses in the following 224.0.0.0 and 224.0.0.255. [3] Both of these addresses are reserved for the network ID and the broadcast address, respectively.

4. MAC Addresses

Each interface on an Ethernet network has one unique MAC address. MAC addresses are physical addresses, unlike IP addresses which are logical addresses. Logical addresses required you to load special drivers and protocols in order to be able to configure your network interface with one or more IP addresses, whereas a MAC address doesn't require any driver whatsoever. It is typically hard-coded into the network card's memory chipset. [4]

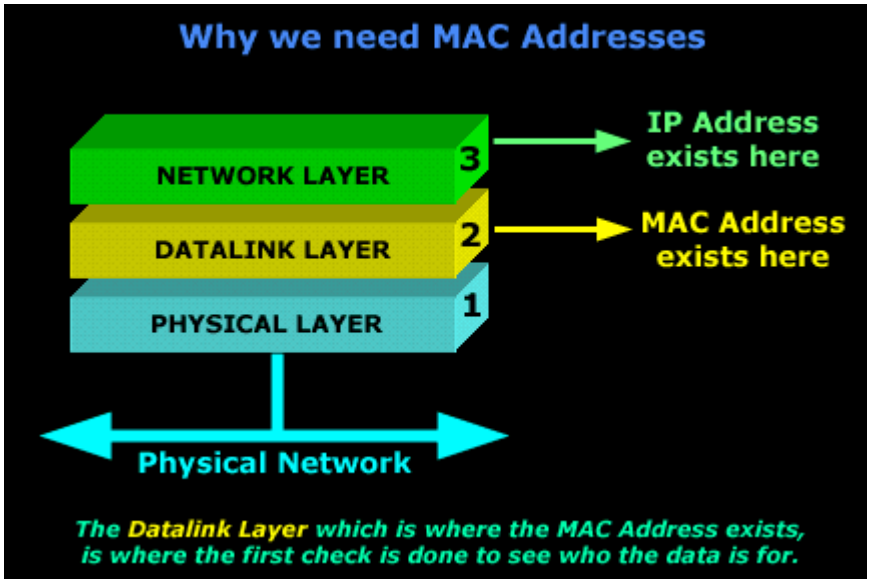


Figure 12. Why we need MAC Addresses (from [3])

To understand why MAC addresses are needed observe Figure 12 above. The Physical Layer understands the electrical signals on the network and uses them to generate the frames which get passed to the Datalink Layer. If a frame is destined for the

computer then the MAC address in the destination field of the frame will match that of the computer's interface adapter. If so, the adapter will accept the frame and pass it on to the Network Layer which, in turn, will check the network address of the packet (e.g., IP address), to determine whether or not it matches a network address to which the computer has been configured. [4]

C. BASIC CRYPTOGRAPHY

The foundation of sending secure information falls into the rubric of cryptography, which is heavily dependent on the field of mathematics. Cryptography in secure network 'collaborative-based' environments can have a large efficiency impact. Understanding the various forms of cryptography is necessary when comparing and contrasting collaborative solutions from an efficiency standpoint. Also, cryptography is critical for information assurance (i.e. data integrity) and user authentication.

The purpose of this section is to familiarize the reader with basic cryptography terms and notations, and to present the main types of cryptography currently employed in network environments.

1. Terms and Notation

Secrecy, Integrity, Authenticity, and Non-repudiation are services provided by cryptosystems. The following list defines these terms along with some other terms associated with cryptography:

- **Secrecy** ensures that information is accessible only for reading by authorized parties.
- **Integrity** ensures that any insertions, modifications, or deletions of data can be detected by the recipient.
- **Authenticity** ensures that the origin of a message can be correctly identified.

- **Non-repudiation** provides that neither the sender nor the receiver of a message is able to deny the transmission.
- **Cipher** is a method for encrypting messages.
- **Plaintext** or **Cleartext**: the original message

  Plaintext P = [p1, p2, …, pn], where p1 through pn represents the plaintext sequence of letters
- **Ciphertext**: the encrypted message

  Ciphertext C = [c1, c2, c2, …, cn], where c1 through cn represents the ciphertext sequence of letters derived from the associated plaintext sequence of letters
- Message M encrypted with key A is denoted as M_A
- **AES (Advanced Encryption Standard)** uses the Rijndael Cipher and supports 128, 192, and 256 bit keys.
- **DES (Digital Encryption Standard)** consists of permutations, binary substitutions (XORing) and a non-linear substitution technique that is implemented by what are called S-boxes (S for substitution). The key length is 56 bits, yielding a key space of 2^{56} unique keys. Due to the processing power of modern day computers, a key length of 56 bits is considered inadequate for security purposes. The lack of security provided by short key lengths prompted introduction of Triple DES, which comes as 2-key Triple DES or 3-key Triple DES (112 bit keys and 168 bit keys, respectively)
- **RSA (Rivest-Shamir-Adleman) Algorithm** is the most common algorithm used in public key cryptography.
- **Hashing** is usually used to determine if a message has been modified. The hash itself is a complicated checksum that is applied to a message,, resulting in unique hashed value. If the hash is applied to a modified message the resulting hash value will be different than the value obtained for the origin message. Hash properties, where H represents Hash:

- **Hash functions:**

  - **MD5 (Message Digest)** - Developed by Ron Rivest (R in RSA). 128 bit hash value. Commonly used on the internet.

  - **SHA (Secure Hashing Algorithm)** - NIST standard. 160 bit hash value.

- **DSS (Digital Signature Standard)** is a NIST standard that is based on public key cryptography. Its application to a message creates unique digital signatures. This standard utilizes discrete logarithms found in SHA for hashing. These digital signatures are electronically analogous to a handwritten signature. Digital signatures not only identify the sender, but also, verify that the digital document was not altered. Digital signatures appear repeatedly in protocols and will most likely be the most common use of cryptography in the future.

2. Types of Cryptography

Conventional and Public Key cryptography are the two main types of cryptography used in today's secure network environments. These types of cryptography are distinctly different. Each has advantages and disadvantages.

a. Conventional Cryptography

With conventional Cryptography, encryption and decryption use the same key. Plaintext is encrypted with the shared key and the ciphertext is decrypted with key it. In comparison to public key cryptography, conventional cryptography is approximately 1000 times faster. [7] However, key distribution proves to be much more difficult and must occur frequently in order to avoid compromise which can allow exploitation.

b. Public Key Cryptography

Public key cryptography was developed in 1976 by Diffie and Hellman. When compared to convention cryptography, public key cryptography is considered to be weaker. Here, each user must generate a pair of keys, a public key and a private key. The private key is kept secret by its owner, while the public key is freely distributed to interested users. Plaintext is encrypted with a private key and the ciphertext is decrypted with public key. Interestingly, both a particular private key and its associated public key are mathematically related and are capable of either encrypting or decrypting. That is, if the private key is used to encrypt a message, then corresponding public key must be used to decrypt the message. Conversely, if the public key is used to encrypt a message, then the corresponding private key must be used to decrypt the message. In this way the key pairs can be used to authenticate the source, when the source's private key is used for encryption, or to protect the data, when the destination's public key is used to encrypt the data.

Public key cryptography is used in many collaborative applications and will be further addressed when comparing collaborative solutions in Chapter 5.

D. BACKGROUND SUMMARY

This section provided an overview of firewalls, multicasting, and cryptography. Firewalls prevent unauthorized access to or from a private network. They can be implemented in both hardware and software, or a combination of both. Firewalls provide logging and auditing functions. Theoretically, there are two types of firewalls: network layer, and application layer. Multicasting involves directing packets to a specific group of hosts. The network hosts can choose whether or not they wish to participate in the multicast group. Multicast group management is typically done with the Internet Group Management Protocol. A typical multicast on an Ethernet network consists of two parts, hardware/Ethernet multicast and IP multicast. Cryptography is the foundation for data secrecy, integrity, authenticity, and non-repudiation. It also provides various levels of

information assurance and user authentication. There are two types of cryptography, conventional and public key cryptography.

Firewalls, multicast, and cryptography are integral to collaborative environments. Chapter Four (Effects of Network Security on Multicasting) and Chapter Five (Comparison of Collaborative Solutions) expand on the importance of firewalls, multicast, and cryptography.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COLLABORATIVE ENVIRONMENTS IN THE DEPARTMENT OF DEFENSE AND INDUSTRY

The exponential growth of the Internet has greatly expanded the potential for online productivity. Realizing the benefit of online productivity, many organizations are seeking software solutions that will increase organizational efficiency. One area that is taking advantage of today's technology is that of online collaboration. Online collaboration significantly contributes to increased productivity and operational synergy of modern day organizations. Widely distributed organizations choosing to remain in a non-collaborative network environment will find themselves left behind as their competitors become more efficient with the use of collaborative solutions.

The intent of this section is to solidify the reader's understanding of collaborative environments. In doing so, a general classification of collaboration and the collaborative process is briefly discussed. More importantly, this section includes examples of collaborative environments that are currently employed in both industry and the Department of Defense.

A. COLLABORATION

According to the Intelligence Community Collaboration, Base Line Study Report, "Collaboration is broadly defined as the interaction among two or more individuals and can encompass a variety of behaviors, including communication, information sharing, coordination, cooperation, problem solving, and negotiation." [10] The act of collaborating in real-time is not a new concept; however, as available bandwidth increases and protocols evolve, new collaborative solutions emerge. Unfortunately, as these solutions become more robust, so does the solution's complexity, which in turn makes choosing a collaborative solution more difficult. Prior to choosing a particular solution, one must understand the process and classification of collaboration and how online collaboration is being utilized.

1. Process of Collaboration

The process of collaborating follows a format of communicating, coordinating, cooperating, and information sharing. [10] Communication occurs through the use of E-mail, audio and video conferencing, telephone, instant messaging, chat, FAX, and/or screen sharing systems. Coordination occurs with the use of tools to support workflow management, calendar and scheduling, and project management. Cooperation is possible with electronic meeting systems, and group authoring software. Finally, information sharing is brought to life through whiteboards, application sharing, knowledge management, and threaded discussions. For example, two users may be interested in a product that is being offered on the Internet. The process of collaborating could include both users communicating in real-time via VoIP (voice over internet protocol) while co-browsing (i.e., the presenter can speak while displaying his/her browser content to the listener).

2. Classification of Collaboration

The previous paragraph introduced several functions of collaboration. These types of collaboration can be generally classified in two areas: asynchronous or synchronous.

a. Synchronous

Synchronous is defined in Merriam-Webster's as "1: happening, existing, or arising at precisely the same time,… 5: of, used in, or being digital communication (as between computers) in which a common timing signal is established that dictates when individual bits can be transmitted, in which characters are not individually delimited, and which allows for very high rates of data transfer". Similarly, synchronous collaborative software allows the files to remain in 'synch' with one another giving the appearance of everyone accessing the same file. That is, no separate copies are created. In a

synchronous environment, all information is current as if it were a master copy. Some examples of synchronous collaborating include: video conferencing, real-time streaming media (video and/or audio) applications, on-line chatting, co-browsing, and instant messaging.

b. Asynchronous

Alternatively, asynchronous is defined in Merriam-Webster's as "1: not synchronous, 2: of, used in, or being digital communication (as between computers) in which there is no timing requirement for transmission and in which the start of each character is individually signaled by the transmitting device". Similarly, asynchronous collaboration does not rely on participants synchronizing their activities. Information to be shared and acted upon is stored in a location accessible by all involved parties without consideration of when others may have modified, stored, or accessed the information. For example, individuals or groups working on a single document are required to merge their revisions to create the newest iteration of the document which is then stored on the host collaboration system. Email and bulletin boards are examples of applications used to support asynchronous communications, while shared calendars can effectively coordinate task schedules. While emails may target individual or clusters of participants, bulletin boards or news groups provide a method of focused discussion on particular topics of interest to larger segments of the collaborating community.

B. INDUSTRY

Business in all sectors of industry is migrating to collaborative tools that complement today's social aspect of online productivity. Through effective collaboration, companies are able to improve their productivity by creating an environment in which work relationships are easily managed, thoughts and ideas are well organized, and project status and deadlines are accurately tracked and represented.

Collaboration in industry is not a new concept; however, software development and technological innovation is changing the medium in which collaboration occurs.

1. Collaboration in Industry

The collaborative functions give a general sense of what is gained through collaborative environments. To solidify what is meant by online collaboration, the following real-world collaborative tools are provided:

- Many building and construction companies along with the Census Bureau development project, Bureau of Alcohol, Tobacco & Firearms (ATF), Amtrak, numerous cities, and other forms of local government use a collaborative solution called Constructware. Constructware is a client-server based application which is a scalable, secure Internet-based project management, collaboration and design management suite that simplifies project management and facilitates online communication among project team members. Toolsets include: personal organizer, reporting, business development, project information, document management, human resources, and design collaboration. [20]
- Ingram Micro Inc., the largest global wholesale provider of technology products and supply chain management services is using the WebEx Enterprise Edition service to deliver Web-based training programs and large-scale project meetings. [24] WebEx Enterprise Edition integrates all of WebEx's advanced Web communication services, WebEx Meeting Center, WebEx Support Center, WebEx Event Center and WebEx Training Center to create a single source for enterprise communications. With WebEx, Ingram Micro associates worldwide have the ability to access Web communications services of the WebEx MediaTone Network from a single login. [24] WebEx provides a range of secure Web communications services designed to meet every business need.

According to a recent industry report, WebEx provides 64% of the world's Web conferencing services and the company was recently named the fastest-growing technology company over the last five years by Forbes magazine. Additionally, with over 7000 companies, WebEx Communications, Inc., is the world's leading provider of Web communications services. WebEx services are used across the enterprise in sales, support, training, marketing, engineering and product design.

- Hewlett Packard and PeopleSoft, Inc. utilize a collaborative solution founded on PlaceWare services. PlaceWare was recently purchased by Microsoft and is now the foundation for Microsoft Offices' Live Meeting. [26] PlaceWare features a conference center which allows an organization to communicate with all their employees, clients or customers, wherever they may be, in a fraction of the time—and at a fraction of the cost—of on-site meetings. [26] PlaceWare Services brings together consulting, education, and other support services in the areas of marketing, sales, eLearning, meetings, and human resources. PlaceWare Virtual Classroom empowers an organization to rapidly train employees, customers and partners, wherever they may be without the costs and inconvenience of traveling. With nothing more than a browser connection, instructors can deliver engaging, interactive training sessions globally.

- The Department of Defense utilizes a system called JOPES (Joint Operation Planning and Execution System. JOPES uses a set of command and control techniques and processes, supported by a computerized information system, to ensure the right amount of timely support gets to the warfighter to ensure a decisive victory. [47] More specifically, JOPES is a combination of joint policies and procedures, supported by automated data processing (ADP), designed to provide joint commanders and planners with a capability to plan and conduct joint military operations [47] in a real-time fashion.

The above examples highlight a few of the many solutions available to organizations that are moving into collaborative environments. The Department of Defense has similar collaborative solutions in place, among others.

C. DEPARTMENT OF DEFENSE

Similar to industry, the Department of Defense is changing the way it utilizes computer technology to carry out its mission. One area of concentration for collaborative environments has been distant learning. The use of higher bandwidth networks, most often the Internet, has come into favor as a way of distributing course materials to students. [19] Although distant learning is not a focus of this paper, it is a significant benefactor of collaborative environments. As such, distant learning, among other forms of collaboration, is included to provide the reader an example of how collaborative software is being used in the Department of Defense.

1. Collaborating in Distance Learning Environments

In geographically separated academic environments, collaboration offers the ability to deliver coursework and learning material to remote students. Not to be mistaken with eLearning type initiatives, which are static in nature (i.e., E-mail, message boards, uploaded files, and/or web sites), these students are able to socialize around academic content and activities promoting an ideal collaborative environment for group projects and dynamic team building. Also, these collaborative environments allow dispersed groups of students to interact in a virtual environment that provides context beyond what is found in emails, message boards, and Web sites.

The Department of Defense's vision is to harness the power of the Internet and other virtual or private wide-area networks (WANs) to deliver high-quality learning. It brings together intelligent tutors, distributed subject matter experts, real-time in-depth

learning management and a diverse array of support tools to ensure a responsive, high-quality "learner-centric" system. [18]

a. Advanced Distributed Learning

Advanced distributed learning leverages the full power of computer, information, and communication technologies through the use of common standards in order to provide learning that can be tailored to individual needs and delivered anytime and anywhere. [18] Advanced distributed learning should not be confused with distributed learning which is centered on media (e.g., tapes, books, CDs, etc) being distributed via mail or other similar methods. Advanced Distributed Learning environments offer a common solution for common problems such as: remote node discontinuity, non-existent real-time/near real-time interaction (e.g., student-to-professor or student-to-student interaction), information distribution. ADL environments offer solutions not only to the military Services and Defense agencies, but to other public-sector organizations, academic institutions, and private industry.

b. Advanced Distributed Learning Initiative

The Department, in the Quadrennial Defense Review (QDR) of 1996, decided to develop a Department-wide strategy to harness the power of learning and information technologies to modernize education and training. The strategy is called the Advanced Distributed Learning (ADL) Initiative, depicted in Figure 13 below.

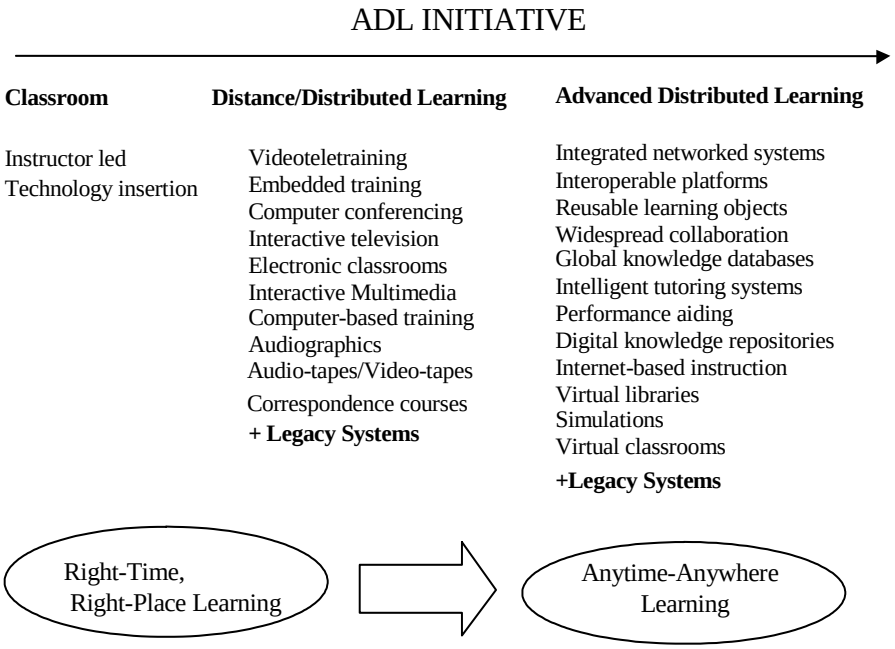


Figure 13. ADL Initiative

c. Advanced Distributed Learning in Application

The following items obtained from the Office of the Under Secretary of Defense for Personnel and Readiness contain examples of how collaboration and Advanced Distributed Learning is being utilized in the Department of Defense.

- The Naval Aviation community is collaborating with General Motors to adapt and re-purpose, for military use in DoD aviation diagnostics and repair, a performance mentoring technology tool which was developed by General Motors for use in its Cadillac division. Performance mentoring allows individuals to improve their work actions through the incorporation of an interactive evaluation system. The objective of this prototype is to demonstrate how COTS technology can be used to provide low-

cost, yet highly effective, on-the-job learning and performance mentoring for H-1 Helicopter maintenance technicians. [18]

- The Defense Acquisition University (DAU) has launched a major initiative to modernize its classroom-based acquisition training by converting to Web-based training using best business practices and industry benchmarks. [18]
- The Joint Staff developed an ADL Initiative Prototype that provides joint doctrine education and training via the Internet. The objective is to infuse high quality joint doctrine to the *Total Force – anytime, anywhere* concept. [18]
- The U.S. Atlantic Command's Joint Warfighting Center (JWFC) of the Joint Forces Command has developed an ADL Initiative prototype in its Joint Distributed Learning Center (JDLC) that can provide JTF Commander and Staff training via the Internet. The objective of the JDLC is to provide a comprehensive source of joint web-based training and review opportunities for command staff members preparing to participate in joint training exercises and real-world operations, in accordance with the joint mission essential tasks of the supported Unified or Specified commander. [18]

d. The Navy's Strategy

The *Navy Knowledge Online* implements a U.S. Navy-wide Distributed Learning System designed to deliver training, education, and information "on demand" as a career-long continuum to support Naval Operational Readiness and personal excellence. [18] Although not collaborative in the sense of streaming media, Navy Knowledge Online provides a central point for many other forms of collaboration among the various Navy communities.

Advanced Distributed Learning initiatives are centered on the Navy's *Strategic Training Vision*, which includes Fleet initiatives, such as *Operational Maneuver from the Sea* and *Network-Centric Warfare* (NCW), a concept for distributed decision-making in the JV 2010 environment. [18] NCW depends on Copernicus, a robust adaptive-bandwidth network architecture that integrates most deployed naval platforms and permits synchronized engagement. Systems that do not migrate to the ubiquitous collaborative environment provided by Copernicus are slated to be retired.

2. The *Groove* Collaborative Solution

DoD also utilizes commercial collaborative solutions, such as Groove. Groove software's unique decentralized architecture provides an agile, secure and extensible collaboration infrastructure to support inter-agency decision-making. The software, which is used by more than 40 government organizations, provides secure communication across unsecure networks, supports mobile users, is self-synchronizing, and Groove isn't vulnerable to attack, because it doesn't have a single point of failure. [23] The following describes two Navy activities employing Groove.

a. Naval Postgraduate School Using Groove Networks

The Naval Postgraduate School (NPS) utilizes Groove as a peer-to-peer collaborative solution. NPS's interest in Groove is two fold. First, NPS conducts research in solutions for establishing distributed, collaborative, command & control centers in decentralized military environments. Second, NPS needs to deliver coursework and a learning environment to the school's primary remote student population. [21] These activities represent implementations of a virtual command center and virtual classroom, respectively.

NPS's primary lecture delivering tool is a Web-based e-learning tool called Blackboard, from Blackboard.com. With Groove, NPS was able to compliment Blackboard by offering synchronous lecture delivery, real-time class interaction, and

interactive question and answer sessions. Remote students are able to synchronously observe the lecture and submit instant messages to which the professor provides a response, addressed to the entire virtual class, via voice messaging. [21] The Groove Workspace's unique features of persistency (e.g., entire chat conversations remain part of the shared space and they're not deleted at session termination) and off-line availability make this collaborative environment highly adaptive to mobile or disconnected users. Here the Groove user is able to work on shared workspace items off-line and during the next on-line period the shared workspace is synchronized with the most current information. Hence, Groove functions both synchronously and asynchronously depending on how it's employed.

The following list contains sponsored Groove related thesis work at NPS:

- Support Complex Humanitarian Aid operations; JFCOM LOE (Limited Objective Experiment); and Virtual Military Operations Center in Hawaii (Pacific Command, U.S. Homeland Security)
- Airborne Collaborative En Route Mission Planning System (SPAWAR)
- SOF UAV Reconnaissance and Surveillance Network (CDTEMS)
- Augmented Reality Network Operations Center (Fleet Transit Experiment)
- Wearable Computing System for Carrier Aircraft Maintenance (Fleet Transit Experiment)
- Ubiquitous Surveillance Network (Homeland Security grant)

b. Navy Physicians Using Groove

In the medical community, an effort to institutionalize a mobile collaborative platform using the Groove solution is supported by the following example: Medical coordinator for Civil-Military Operations, CDR Eric Rasmussen, is using

Groove to communicate with 45 co-workers via encrypted instant messages, and any file changes he makes are securely updated, no matter how little bandwidth he has. [22] Tools used in this application of Groove include: incident alerts, casualty reporting, evacuation requests, refugee registration and screening, map annotation, plus others.

3. The WebEx Collaborative Solutions

Computer Technology Services, Inc. (CTS) offers the U.S. Government market Web meeting and training via WebEx Communications Inc. services. WebEx enables government agencies to expand their reach, accelerate time-critical communication, reduce travel costs and improve productivity by holding interactive meetings through the Web. WebEx services enable secure data, voice and video communications through the browser and are supported by the WebEx MediaTone Network, a global network specifically designed for high-speed Web communications. [25]

Computer Technology Services, Inc has a global network that places WebEx in a unique position to leverage the increasing government demand for Web communications services. Like commercial business, Web meetings have become a standard part of government communications because they dramatically reduce travel costs, increase productivity and improve communications [25]

D. SUMMARY

This section covered several forms of collaboration and how collaboration is generally classified as being synchronous or asynchronous. The section also presented real-world examples of collaborative environments found in both industry and the Department of Defense.

It's important to understand that prior to implementing a collaborative solution; an organization must overcome any end-user social and/or cultural barriers surrounding collaborative adaptation. Human beings are habitual and have a tendency to resist

change. Resistance can result from many cultural norms, learned behavior, organizational ‘status quo’ etc. In the area of security, information sharing policies need to be formulated. These policies will greatly vary in complexity and flexibility, as determined by the organization. Finally, in an organization’s network infrastructure, both intra-domain and/or cross-domain, there may exist networking components that could impede implementation of a collaborative solution. Some of these concerns are addresses in the next section which covers network security in multicast environments.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EFFECTS OF NETWORK SECURITY ON MULTICASTING

The necessity of auditing, logging, and controlling data flow for security reasons is understandable in today's high threat network environments. However, with the advent of new collaborative applications that utilize high bandwidth features such as streaming video, efficient multicast transmissions will be a cornerstone in determining network effectiveness. Redefining the use of firewalls in multicast environments will allow an organization to optimize available bandwidth. This section addresses the role of multicast security differences, multicast firewalls, tunneling, bandwidth management, efficiency costs of authentication, and effects of multicast on the NPS firewall.

A. MULTICAST SECURITY DIFFERENCES

Securing multicast communications is unlike securing unicast communications. That is, one-to-one authentication (i.e., unicast) is available via standard mechanisms [15], where as, one-to-many or many-to-many authentication (i.e., multicast) is more complex and does not benefit from standard authentication mechanisms. Other differences include:

- multicast transmissions involve arbitrary data size and varying sets of participants
- security of multicast is based not upon its participants, but instead, upon its data (i.e., multicast communication is authenticated by authenticating packet data) [17]
- Multicast source authentication is required in order for a user to trust the authenticity of the received data stream. Source authentication allows the receiver to ensure that the received data is authentic, even when none of the other receivers of the data is trusted. [15]

B. ROLES AND EFFECTS OF THE MULTICAST FIREWALL

The role of a typical firewall is to filter network packets based on some predefined criteria, controlling access to certain network resources. [11] Like typical firewalls, multicast firewalls operate in conjunction with routers at the network layer of the OSI model. However, multicast data passing through a multicast firewall utilizes special MAC layer addresses to perform its task and can be easily identified via their MAC addresses. The effect produced from multicast firewalls results in more efficient processing of packets at the Data Link Layer of the OSI model. [11] Increased efficiency is a product of the frames being handled in the hardware relieving the CPU of performing layer three actions such as, interrogating addresses. The multicast firewall provides real-time control over bandwidth usage and management capability; thereby, reducing conflict with non-multicast traffic.

1. Multicast Firewalls Functions

Multicast firewalls perform: a) multicast packet forwarding in place of tunneling across existing routers for an Intranet, b) packet replication optimization via multicast group membership management (multicast spanning tree management), and c) subnet bandwidth management, by assigning priorities to multicast addresses and filtering (dropping) packets for each group according to specified criteria. [11]

2. Firewall Multicast Security Policy

The multicast security policy involves specifying UDP ports that correspond to a set of allowed multicast groups that are candidates to be relayed across the firewall. [17] Policies can be supported by: [17]

a. Static configuration

Candidate groups/ports are configured in advance

b. Explicit dynamic configuration

Based upon an explicit request from one or more trusted clients, the set of candidate groups/ports could be set and updated automatically

c. Implicit dynamically configuration

Based upon the contents of some pre-authorized multicast group/port, the set of candidate groups/ports could be determined implicitly. For example, suppose a security policy decides that the default MBone SAP/SDP session directory may be relayed, as well as any sessions that are announced in this directory. A 'watcher' process, associated with the firewall, would watch this directory, and use its contents to dynamically update the set of candidates [17].

3. Relaying Candidate Multicast Groups

If a multicast group becomes a candidate to be relayed across the firewall, the actual relaying should not be done continually. It should be done only when there is actual interest in having this group relayed. [17] From a bandwidth perspective, it is inefficient if there is no interest in having the group relayed. Also, relaying unwanted multicast groups unnecessarily tasks the firewall's resources.

a. Determining When to Relay

The best way for the firewall to determine when a candidate group should be relayed is for it to use actual multicast routing information, thereby acting much as if it were a real inter-domain multicast router. [17]

- For single subnet intranets, the firewall could listen for IGMP requests to learn what and when a candidate group has been joined by a node
- Or, a firewall could periodically ‘probe’ each group to see what groups have recently joined
- Or, a firewall could be explicitly notified by each node when it joins or leaves a multicast group

It should be noted that the duplication of multicast routing functionality makes probing and explicit notification undesirable and scale poorly for large networks.

b. Relaying Mechanism

The actual relaying mechanism that’s used to relay multicast packets will depend upon the nature of the firewall. For cross-firewall relaying, placing a bandwidth limit will circumvent a ‘denial of service’ attack which could flood a multicast group with garbage. [17]

The multicast firewall is introduced in order to overcome the bandwidth bottleneck and address the fundamental concern of deploying such applications – that they use up significant network bandwidth, sometimes to the detriment of existing data applications. [11] This device operates in parallel with existing routers to provide routing and bandwidth management of multicast traffic used by multimedia applications. Figure 14 below depicts a multicast firewall used in conjunction with several existing routers.

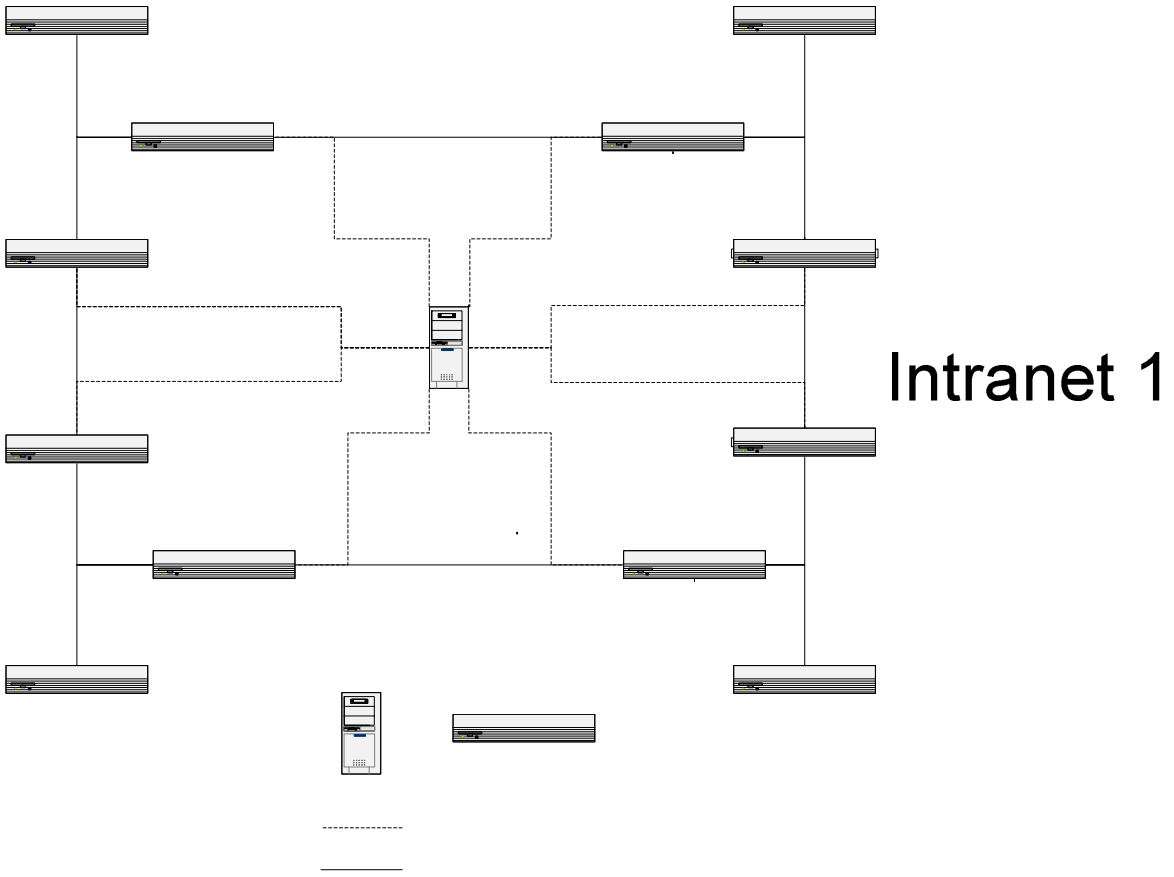


Figure 14. Firewall used as a Multicast Relay Mechanism

C. EFFECTS OF TUNNELING

Tunneling has been the preferred method of conducting secure unicast transmissions. The advent of multicast has introduced additional complexity and tunneling is one of the ways to support multicast applications throughout a corporate enterprise intranet with non-multicast capable routers. [11] For tunneling to occur, a tunneling device is placed in each LAN for the purpose of receiving multicast packets, encapsulating the packet into a unicast packet to send it through the router to the tunneling device on the other LAN which would then un-encapsulate it for retransmission. [11] Unfortunately, this method incurs significant bandwidth in order to support a given multimedia stream, as well as defeating the purpose of multicasting in

that separate streams must be generated for each tunneled connection. The effects of tunneling can have a severe impact on network efficiency when attempting to conduct a one-to-many or many-to-many multicast. This is the technique used in the MBONE to support multicast across the existing Internet.

1. Effects of Tunneling

Multicast tunneling, while effective, introduces additional bandwidth requirements. [11] If forced into a tunneling scheme, UDP-based tunneling should be utilized vice TCP-based tunneling. UDP-based tunneling is a better fit for relaying multicast packets and if congestion avoidance is a concern, then the tunneled traffic could be rate-limited, perhaps on a per-group basis. [17] Other effects include, [11]

- Lack of multicast capable routers in most private internets constrains the deployment of multicast applications
- The cost of implementing tunneling to forward multicast packets among the various subnets may not be acceptable if several multicast applications are active simultaneously
- Lack of Quality of Service (QoS) capabilities in current contention-based networks (e.g. Ethernet) may result in multicast data consuming all available bandwidth in each subnet, causing network congestion

2. Tunneling Alternative

Instead of utilizing a tunneling device to process multicast packets, a firewall may be placed in parallel with the router to interconnect two or more subnets requiring multicast support. [11] This method allows the router to forward unicast packets while the firewall will forward multicast packets. Normally, firewalls use Layer 3 processing techniques; however, multicasting utilizes specific Layer 2 address formats that are clearly distinguishable from other types of traffic can therefore be used to perform packet

forwarding processing within that layer. [11] Additionally, a firewall with N ports will function as N tunneling devices for N interconnected LANs. [11]

D. BANDWIDTH MANAGEMENT

Regarding multimedia, bandwidth management can be categorized as a basic form of QoS enforcement [11] where both multimedia and other data traffic have limits set for the percentage of bandwidth consumed.

1. Multimedia Applications

Multimedia applications, which typically utilize multicast transmission, are able to tolerate some data loss. This toleration allows bandwidth management to enable such applications to share available network resources instead of requiring that a new network be setup solely for multimedia traffic. [11]

2. Prioritization of Multicast Addresses

The prioritization of multicast addresses provides additional control over the usage of the allotted multicast bandwidth. Higher priority applications, such as video conferencing, could be assigned a particular multicast address and be provided better QoS compared to lower priority applications, such as delivery of non-time sensitive data. [11] Consequently, traffic within a given priority that exceeds the maximum threshold would be dropped, there by limiting its impact on higher priority traffic.

3. Multicast Group Management

Multicast sessions across different subnets are established by using gatekeepers, which are found in H.323-based system architectures, or by the Internet Group

Management Protocol (IGMP), found in MBONE configurations. [11] H.323 is an international standard for IP Telephony and IP-based video conferencing.

a. Tree Growth and Pruning with a Multicast Firewall

While each network subnet is only one hop away from the multicast source via the firewall, the bandwidth requirement for the multicast firewall for tree growth and pruning is limited to control packets to and from the firewall itself. [11] Additionally, multicast tree optimization is greatly simplified since the packet forwarding is performed internally to the firewall. Performing the group management and multicast tree optimization within the firewall eliminates the network overhead associated with spanning tree creation and protocol packet forwarding inherent to DVMRP and MOSPF that were designed for operation on the Internet rather than an enterprise intranets. [11][12]

b. H.323 Based System with a Multicast Firewall

In H.323 type architectures, gatekeepers are tasked with the management of session members using H.225 signaling [11][12][13] From an efficiency standpoint, a multicast firewall's tree optimization complements the zone and call management functions of the gatekeeper. [13]

c. Multi-hop Management Traffic

In both IGMP and H.323 based systems, the network overhead is similar, since no multi-hop management traffic is generated as inter-subnet connectivity is handled within the firewall itself. [11]

4. Bandwidth Management Components

Bandwidth management components consists of: a) usage policies that address multicast traffic prioritization, b) sampling mechanisms to determine the current network load of each subnet, and c) filtering mechanisms that implement the policy based on the sampled network load for each subnet. [11]

The multicast firewall takes advantage of the ability of multimedia applications to tolerate packet loss to perform its bandwidth management function. As such, the bandwidth management capability of the multicast firewall is not intended for guaranteeing multimedia application QoS. Rather, it is to provide reasonable QoS for multimedia applications by preventing multicast traffic from overwhelming the capabilities of the network to carry both normal and multicast traffic. [11]

5. Bandwidth Usage Policy

The bandwidth usage policy defines the lower and upper subnet bandwidth thresholds for which multicast bandwidth management will be enabled. [11] Instead of competing with other applications for bandwidth that is insufficient for multimedia application usage, the firewall stops inter-subnet multicast forwarding until subnet traffic returns to a normal level. Between the two thresholds, there is graceful degradation of QoS for multicast applications defined by this Multicast Traffic Priority policy. [11] The Multicast Traffic Priority, explained above, may further divide the available bandwidth into several priority thresholds.

This bandwidth usage policy can be managed dynamically by the H.323 gatekeeper to fine tune allocated bandwidth for inter-subnet multicast data streams. Additionally, the multicast firewall extends the basic bandwidth control offered by H.323 (request, confirm and reject handshakes) with multicast priority features. [11]

6. Bandwidth Sampling Mechanism

The bandwidth sampling mechanism determines the level of traffic on each subnet. This is achieved by placing a Network Interface Card (NIC) into promiscuous mode in order for the firewall to receive every packet in the subnet. This provides the bandwidth and prioritization filters with the necessary data to make drop/forward decisions regarding multicast traffic. [11]

E. EFFICIENCY COSTS OF AUTHENTICATION

Signing each data packet provides good source authentication; however, it has high processing overhead for signing and verifying the data, and increased bandwidth usage for forwarding the signatures with the data. [16] Signature verification is computationally expensive [16], making it even more susceptible to IP multicast denial of service attacks.

1. Authentication Schemes

A number of schemes have been introduced to solve the multicast authentication problem [16], two of which are:

a. TESLA (Timed Efficient Stream Loss-tolerant Authentication)

TESLA uses only symmetric cryptographic primitives such as pseudorandom functions (PRFs) and message authentication codes (MACs), and is based on time-release of keys by the sender. [16] In this scheme, the sender uses a regular signature scheme to sign the initial commitment, while all subsequent packets are authenticated through chaining.

b. EMSS (Efficient Multi-chained Streamed Signature)

EMSS is based on signing a small number of special packets in a data stream. Each packet is linked to a signed packet via multiple hash chains. The hash of each packet is appended to a number of subsequent packets. [16]

Both of these authentication schemes purport low computation overhead and tolerate arbitrary packet loss. [16]

2. Multicast Key Management

As multicast progresses, secure multicast sessions will be a requirement for scenarios such as wargaming, law enforcement, teleconferencing, command and control conferencing, disaster relief, and distributed computing. [14] A key problem is enabling each user to determine/obtain the appropriate security key in order to access a particular group without permitting unauthorized parties to do likewise, as well as, securely rekeying the users of the multicast group as necessary. [14]

Several architectural issues exist regarding implementing an effective key management program. These include strength of security, cost, initializing the system, policy concerns, access control procedures, performance requirements, and support mechanisms. Some solutions are presented in [RFC2627]; however, in the area of performance requirements, the hierarchal tree approach [14] for key distribution provides desirable storage and transmission efficiency.

a. Hierarchal Tree Approach

The Hierarchal Tree Approach balances the costs of time, storage, and the number of required message transmissions, while using a hierarchical system of auxiliary keys to facilitate distribution of new Net Keys. The common multicast group Net Key allows multiple users to share the same security attributes and communication requirements to securely communicate with every other member of the multicast group.

[14] The efficiency gained in the storage and transmission is at the expense of additional server processing requirements. [14]

F. NAVAL POSTGRADUATE SCHOOL'S FIREWALL AND MULTICAST

The Naval Postgraduate School currently employs two application-based 'stateful' Symantec Enterprise 7.0 firewalls. Both firewalls are placed in parallel between an internal and external switch followed by an internal and external router. Figure 15 below depicts the NPS firewall topology.

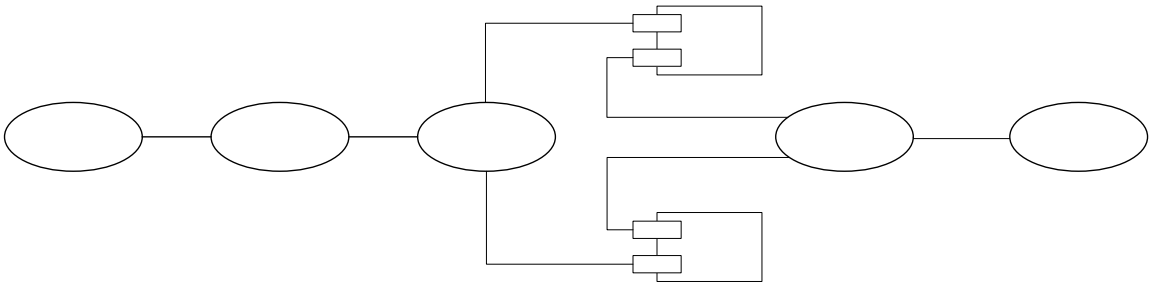


Figure 15. NPS Firewall Topology

Neither firewall is configured to handle multicast protocols. However, both firewalls incorporate third generation security proxies and packet filtering. In addition, they feature built-in protection against Denial of Service (DoS) attacks and integrated, blended threats. [43] The firewalls also support inbound and outbound Network Address Translation (NAT) for both VPN and non-VPN traffic. By default, this shields internal addresses from outside viewing. [43] From an efficiency standpoint, the firewalls support the integration of both hardware and software high-availability and load-balancing mechanisms. [43] The firewalls allow administrators to implement and enforce corporate network policies, such as access to certain servers, access to certain file shares, and

access limited by time period. They also contain configurable items for both users and user groups. [43] Symantec Enterprise Firewall 7.0 is EAL-4 certified. [43] The EAL certification involves an evaluation to certify that a product meets claims for cryptographic support as defined by the Common Criteria for Evaluation Assurance Level 4 augmented (EAL-4). This certification is granted by the U.S. Government National Institute of Standards and Technology (NIST) through the National Information Assurance Partnership (NIAP). [39]

An upgrade to Cisco's PIX 6.2 firewall is scheduled this spring. The Cisco PIX 6.2 firewall will be able to handle significantly higher throughput for branch office environments using broadband connectivity. [44] New features include PPP over Ethernet protocol, ISP compatibility in small office/home office networks, and the same unified VPN client framework found in other Cisco VPN solutions. [44] The PIX OS also comes with improved IP telephony and multimedia services that include Port Address Translation, and several options for communication with Cisco IP Phone and Cisco IP SoftPhone products. [44] This last improvement provides a significant enhancement for bandwidth intensive streaming multimedia applications.

In the area of multicast, Cisco's PIX 6.2 firewall will provide multicast support, using IGMPv2 and Stub Multicast Routing. The PDM version 2.0 enables you to statically configure multicast routes or use an IGMP helper address for forwarding IGMP reports and leave announcements. It's multicast support includes: [45]

- Access-list filters that can be applied to multicast traffic to permit or deny specific protocols and ports.
- NAT and PAT (Port Address Translation) that can be performed on the multicast packet source addresses only.
- Multicast data packets with destination addresses in the 224.0.0.0/24 address range are not forwarded. However, everything else in the 224.0.0.0/8 address range is forwarded.
- IGMP packets for address groups within the 224.0.0.0-224.0.0.255 range are not forwarded because these addresses are reserved for protocol use.

- NAT is not performed on IGMP packets. When IGMP forwarding is configured, the PIX Firewall forwards the IGMP packets (report and leave messages) with the IP address of the helper interface as the source IP address.

It should be noted that the PIX Firewall, nor any other available firewall, is unable to contain multicast traffic storms, regardless of packets origination (internal or external). A network storm is an error condition resulting from: faulty protocol implementations, undetected network loops, or faulty network equipment that can significantly disrupt attached stations. The storm consists of repeated transmission of a high rate of broadcast (or other multicast) packets onto the network. However, there are switches, such as the SuperStack II Switch 2200, that have mechanisms that contain multicast packet firewalls which limit the rate at which multicast packets are forwarded. This limitation is accomplished by allowing the adjustment of the threshold rate; thus, controlling the effects of multicast storms on a network. [48]

G. COLLABORATION SUMMARY

This section addressed the role of multicast firewalls, tunneling, bandwidth management, multicast security differences, efficiency costs of authentication, and firewall specifics at NPS. With multicast firewalls, packet forwarding in place of tunneling occurs. Packet replication optimization via multicast group membership management also occurs. Subnet bandwidth management is the last item performed by multicast firewalls. Tunneling effects and tunneling alternatives were discussed. Bandwidth management addressed usage policies and sampling mechanisms. Multicast security differences and cost of authentication were also discussed. Finally, NPS firewalls and multicast capabilities were identified.

V. COMPARISON OF COLLABORATIVE SOLUTIONS WITH A FOCUS ON SECURITY

As many emerging technologies develop, a variety of implementation methods normally result. The mechanisms delivering the technology often result in a plethora of options for the end user. Although collaborative environments have been in existence for some time, the technology that delivers collaborative solutions is approaching new highs. Available collaboration solutions are abundant and can be found with numerous features serving the casual home user all the way to the largest of enterprises. Today's collaborative solutions provide services ranging in robustness, applicability, security, and ease of implementation. Collaborative technologies and solutions are in a continual development phase. Unfortunately, as with any new technology and/or solution, not only must the customer be wary, but also the developer. On one hand, the customer is faced with understanding the collaborative needs and/or requirements that best fit their organization. On the other hand, the collaborative developer is faced with understanding the needs of the customer and the limitations of the internet infra-structure and/or developing standards. This understanding of needs coupled with a fast paced technology industry, makes for an interesting topic of comparing collaborative solutions.

This section provides an in-depth comparison of collaborative solutions. More specifically, it points out the existence of numerous solutions then describes the various aspects that should be considered when selecting a collaborative solution (i.e. network architecture, security, and efficiency). The intent of this section is not to select the best possible solution through an unrealistic, exhaustive analysis of each available collaborative tool, but to impart upon the reader areas of concentration that will assist in selecting a collaborative tool that fits a particular organization.

A. COLLABORATIVE SOLUTIONS

There are a plethora of collaboration tools available. With that said, it is important to recognize that some tools are not built using common industry standards and

some do not support a dynamic network infrastructure. In addition, some solutions are more interoperable than others (i.e. they're able to integrate seamlessly into the current network environment). Migrating to collaborative environments inevitably causes a social change in the way an organization conducts day-to-day business. Regardless of the how a collaborative technology is delivered to an organization, the social change, coupled with a possible learning curve associated with the collaborative environment, will greatly affect the initial use of a collaborative solution.

The following list contains a small selection of the collaborative solutions available. Each of these solutions has their advantages and disadvantages, and depending on an organization's architecture (discussed below in Section C), some are better suited than others.

Next Page	PlaceWare
Endeavors Technology	WebX
Groove	Centra
Constructware	B.efficient
EZmeeting	CommunityZero
Looking Glass	Mayeticvillage
Horizon Live	Adrenamail
SharePoint	Communicast

PlaceWare, WebX, Groove, are some of the large collaboration developers. Large enterprise systems like WebEx, Microsoft Office Live Meeting (formerly PlaceWare) and Centra can be effective for large institutions and international organizations that need to run large meetings and conferences online with attendants in the hundreds or with large training infrastructures and complex logistic needs. Another collaboration tool, more suited to smaller workgroups, is Groove which has a slightly different approach to collaborative solutions found in distributed large enterprises.

Groove's collaborative approach was briefly described in Chapter 3 and will be described in more detail throughout this chapter.

In the next section, an avenue of comparison is presented. More specifically, the comparison will encompass collaborative features, architecture, security, and efficiency. Each comparison area concludes with a real-world application/example. In most cases, these applications/examples will consist of Groove, Microsoft Office Live Meeting 2003, and/or WebX. Many of the other collaborative solutions mirror both of these products and provide their own flavor to collaborative environments. However, Groove is selected because of its relevancy to the Naval Postgraduate School and several other DoD activities named in Chapter 3. Microsoft Office Live Meeting 2003 is selected because of its potential ubiquitous deployment throughout DoD. WebX is selected due to its predominance in global web based collaboration.

B. COLLABORATIVE COMPARISON

While comparing and contrasting available collaboration tools, an organization is faced with choosing a solution that is robust enough to fit an organization's needs, yet secure enough not to compromise the organization's network security.

Here, the end user is faced with deciding on which solution is the right solution. The most significant factors surrounding the use of collaborative solutions are:

1) Knowing how a particular collaborative solution will benefit an organization,

2) Understanding implications on collaboration due to various network architectures,

3) Understanding the necessity and impact of network security requirements, and

4) Understanding the protocols and technology that efficiently use bandwidth.

1. Collaborative Features

Before delving into collaborative architecture, security, and efficiency, basic features of Microsoft Office Live Meeting 2003, Groove, and WebX will be presented.

a. Microsoft Office Live Meeting 2003

Microsoft Office Live Meeting 2003, formerly PlaceWare Conference Center, and Microsoft Office Live Communications Server 2003, formerly Microsoft Office Real-Time Communications Server 2003, are distinct yet complementary offerings, so it is fitting that they share a consistent naming convention. [29] Since PlaceWare is the primary collaborative tool of Microsoft Office Live Meeting 2003, features unique to PlaceWare will be presented.

Enterprise customers prefer PlaceWare web conferencing because of its scalable, reliable and secure browser-based architecture, which is based on technology developed and tested at Xerox PARC. The company offers unparalleled performance for all types of web-based communications, from large-scale meetings with up to thousands of attendees, through small collaborative meetings, presentations, and e-learning sessions. Founded in 1996, PlaceWare has already attracted more than 3,100 leading organizations that see web conferencing as a natural evolution in helping their businesses compete more effectively in the global marketplace. [29] In addition, PlaceWare is the only web conferencing provider that is flexible enough to deliver tailor-made online services for both small collaborative meetings and large-scale events or conferences. PlaceWare is also the only web conferencing provider to offer two unique Virtual Environments, Auditorium Places and Web Meeting Places, within a single web conferencing service. [30] Auditorium Places is designed to host large-scale, structured events and conferences, featuring a Q&A Manager that allows multiple moderators to handle questions while freeing the presenter to focus exclusively on delivering the presentation and an Audience Seating Chart and Mood Indicator that allow your audience to interact during the meeting and provide instantaneous feedback to the presenter without disrupting the presentation for the other attendees. [30] Web Meeting Places is designed to replicate the highly collaborative work environments of small meetings, featuring collaborative annotation tools, application and desktop sharing, private chat capabilities and more. [30] Both of these environments are delivered under the umbrella of a single service with a common

URL, a shared meeting calendar, streamlined user management and administrative reporting. [30]

PlaceWare's availability allows presenters to present from their own desktop or store materials on PlaceWare's highly secure network. Once content is uploaded to the PlaceWare site, presenters can log on from any system. And presenters can always go back to a meeting or event to reuse materials, see notes that they created, or edit presentations. [30] At any time in the meeting, presenters can open and present a document, or demonstrate an application to remote participants, a capability that offers flexibility, mobility and total security. Security that is founded on access controls, meeting keys, and industry standard 128-bit RC4 SSL encryption for data transmission. [30]

PlaceWare's Developer Integration Support APIs allow its customers to create completely custom Conference Center front-ends to schedule meetings, conduct queries and searches, alter meetings, and report meetings [30]. The APIs allow experienced developers to quickly and easily create a front-end to the PlaceWare system. [30] In the near future, organizer creation APIs will allow end users to synchronize users and members with pre-existing directory and LDAP servers.

PlaceWare's reply service, One-Touch Recording & Playback, allows organizations of all sizes to quickly and easily record any session without the need for special hardware or software. Replay captures every aspect of the live session including: PowerPoint slides and annotations, live demonstrations of applications, audience polls, text and whiteboard slides, and web pages. An end user can also capture audio on the PlaceWare server without special telephony equipment. The software simply calls into the conference line or directly to an individual's telephone to record the audio portion of the session. Following the session, the presenter can provide a link to the high-quality recording, which is streamed from PlaceWare's servers and displayed using Microsoft Media Player, a standard application that ships with Windows. [30]

b. Groove

Groove provides a unique collaborative environment of shared spaces, file sharing, joint editing and viewing. It allows the end user to create secure interactive *shared spaces* where information, people and tools are brought together to get the job done. Shared spaces reside on each participant's PC. Work done in the space by one 'member' is instantly seen by all members. End users are able to work in the space together, or work offline, returning to the space over time. Groove keeps all members' PCs updated with the latest changes. [32] With Groove, all files are securely shared with anyone who is a member of the shared space regardless of a member's location. Files are always of the latest version with no size limitations. In addition, live joint editing of Word documents is possible along with live joint viewing of PowerPoint slides.

Groove is built for the way people work. It includes text- and voice-based instant messaging plus a wide assortment of tools and toolsets for sharing content of all kinds, working together, and managing projects and meetings. Groove deploys immediately as a group application, with a common set of project and meeting management and file sharing tools for business activity. Users choose how they communicate and work; selecting tools that match their interaction style and make the most sense for the tasks at hand. Groove integrates with and extends the capabilities of familiar communication and business productivity applications, including Microsoft Office, SharePoint Team Services, Outlook, Windows XP, Messenger, and Project. [33] It allows more effective, contextual, dynamic interaction and permits greater end-user control. Like many other collaborative solutions, Groove provides richer context, immediate feedback and real-time interaction. Users always have access to content and functionality of the application regardless of network connectivity. Finally, Groove gives secure, direct access to information and people. [33]

Groove has the ability to work offline. End users can continue to work while disconnected from the Internet (i.e. all their changes will be updated automatically to all members upon reconnection, keeping other users up-to-date even when they are not online at the same time) Groove also has the quality of persistence. Content changes to shared spaces are automatically saved. Hence, the latest content is always available for review and updating by shared space members. Groove performs real-time updates. All

changes made on one user device immediately appear on all other online users' devices. There is no need for users to "refresh" a shared space while online. [33]

Groove has a level of awareness and comprehension. Users can tell at a glance whether their contacts are online, and within shared spaces, whether they are active, what their roles and permissions are, and what they are doing in the space. Groove is comprehensive. Unlike collaboration products that offer single functionality, such as file sharing or searching, Groove Workspace offers a full range of interactive tools and toolsets and a complete collaboration environment that's built upon a robust extensible platform for which new tools and toolsets can be built. [33]

Recently, the Joint Interoperability Test Command said Groove v2.5 satisfies their 14 interoperability requirements. The Department of Defense (DoD) certification for collaboration interoperability was obtained by Groove's Workspace version v2.5 in conjunction with version 2.0 of the DoD Defense Collaboration Tool Suite (DCTS), a standards-based means for collaboration among the U.S. defense and intelligence communities. DCTS evolved from a 1999 congressional mandate to the U.S. defense and intelligence communities to address the lack of interoperability among their collaboration tools. The mandate: Develop a strategy for implementing collaboration tools throughout the DoD, and validate a prioritized list of functional requirements for DoD collaboration tools. [23] DTCS provides voice and video conferencing, document and application sharing, instant messaging and whiteboard functionality to support defense planning. DCTS, which takes advantage of commercial off-the-shelf software, gives U.S. military and intelligence personnel the ability to link various command, control, communications, computers and intelligence systems for sharing data, conducting collaborative planning, and consulting on information from worldwide locations. [23]

c. WebEx

From a government perspective, WebEx enables government agencies to expand their reach, accelerate time-critical communication, reduce travel costs and

improve productivity by holding highly interactive meetings through the Web. WebEx provides an efficient way to conduct vital communications throughout the country and around the globe. More specifically, WebEx services enable secure data, voice and video communications through the browser and are supported by the WebEx MediaTone Network, a global network specifically designed for high-speed Web communications. [25] According to a recent industry report, WebEx provides 64% of the world's Web conferencing services and the company was recently named the fastest-growing technology company over the last five years by Forbes magazine. [25]

WebEx provides a wide range of secure Web communications services designed to meet every business need. Based on the unique communications capabilities of the WebEx MediaTone Network, WebEx Training Center blends data, voice and video communications to create an engaging online environment that simulates face-to-face training. Trainers can interact with attendees, share streaming media modules, use live video and demonstrate applications, even passing control to attendees. After the session, WebEx Training Center's advanced recording and editing functionality allows trainers to create valuable digital libraries of training sessions. In addition, the WebEx Training Center is an open service platform, allowing partners and solutions providers to integrate with the service. [25]

The WebEx MediaTone Network is the only carrier-class network specifically designed to deliver the rich multimedia online meeting and Web conferencing services required to meet the global communications needs of the enterprise. It delivers optimal performance by routing communications across several WebEx switching centers. The result is a high-performance network that provides unmatched levels of service integration, security, personalization and performance.

The WebEx MediaTone Network also integrates a highly scalable software and API architecture specifically designed for optimized delivery over distributed networks. [25] This carrier-class software infrastructure supports the full range of data, voice, and video interactivity needed to enable dynamic, real-time online meetings. [25]

2. Collaborative Network Architecture

The architecture surrounding a collaborative solution will, in varying degrees, either compliment the collaborative environment or cause conflict at every step throughout the collaborative process. The challenge surrounding network architecture is how to establish effective collaboration, not only within the corporate network but also across the Internet. In the recent past, there have been major collaborative architectural inconsistencies. For example, Microsoft's SharePoint Server (SPS) was built on the Exchange-derived Web Storage System, while SharePoint Team Services used SQL Server and the Windows file system for its storage. In terms of architecture, they didn't share much more than a first name, [9] that is not very collaborative. The architecture of the Internet is similar to the architectures of large organizations. For example, democratic governments are normally highly centralized organizations while many terrorist organizations are normally highly-decentralized organization. Both have pros and cons for carrying out their organizational objectives.

a. Architecture Classifications

Like real-world governments, network architectures are similarly classified into centralized, decentralized, and/or hybrid architectures

- ***Centralized Architecture***

  Like the United States with its centralized governmental foundation, a centralized network will control (or at least attempt to control) events that occur in its environment. Centralized policies and objectives are strictly enforced. Changes to the network environment are closely monitored with intrusion detection devices. Firewall rules effect transiting data that is either 'allowed' or 'not allowed' access to or from the network. All users are centrally authenticated giving a level of assurance regarding the identity of the user. From

a security perspective, a centralized architecture can be very secure and offers the most control over intranet users.

- ***Decentralized Architecture***

Regarding the decentralized network architecture, there are no central policies or objectives to be enforced. This architecture is ideal for a largely distributed organization. It is much more nimble and flexible, resulting in an environment that is extremely conducive for collaboration. However, decentralized networks have greater security risks.

- ***Hybrid Architecture***

In the hybrid architecture, the network combines characteristics and features of both centralized and decentralized architectures. As determined by an organization's needs a proper architectural balance between centralization and decentralization results in an effective networking solution.

b. Architecture in Application

Microsoft Office Live Meeting 2003 – Figure 16 below depicts the lineage of the SharePoint family. OSPS (Microsoft Office SharePoint Server) is entirely built on WSS (Windows SharePoint Server); one of its primary functions is to aggregate and search WSS sites. [9] WSS is built on the .NET Framework, stores data and metadata in SQL Server, and OSPS 2003 relies on BizTalk Server for enterprise application integration. [9]

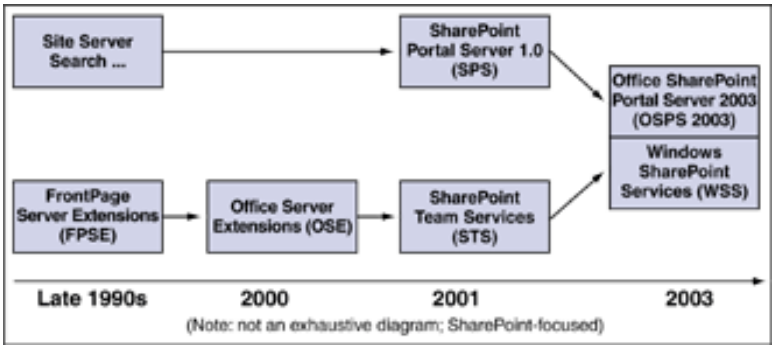


Figure 16. SharePoint Lineage (from [9])

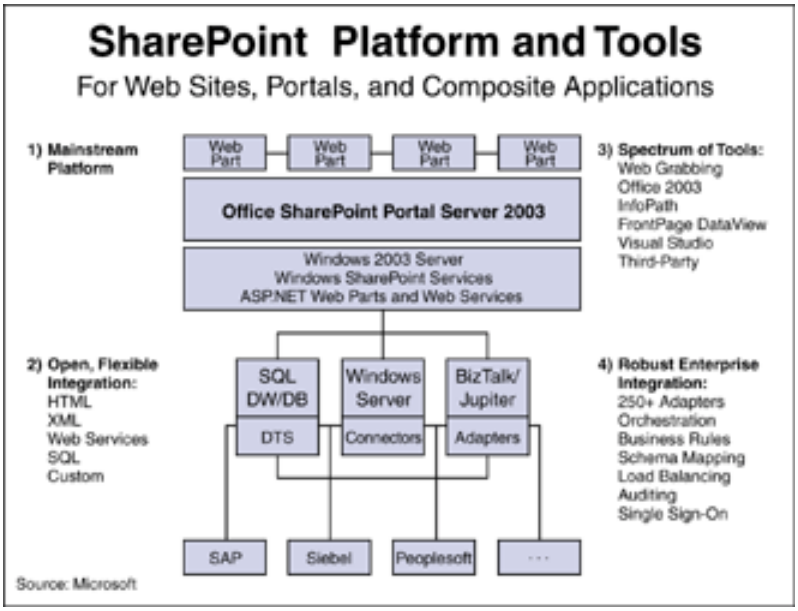


Figure 17. SharePoint is part of constellation of collaborative tools and technologies (from [9])

Figure 17 above shows the SharePoint Portal Server 2003's platform and tools. With Office SharePoint Portal Server 2003, end-user productivity tools range from collaboration and content/document management to portal-style access to SAP, PeopleSoft, Siebel, and other back-end resources. [9] With WSS and .NET, applications can be extended with a wide range of collaborative services. One of which is Microsoft Office Live Meeting 2003's PlaceWare features. PlaceWare's network architecture maintains more than 150 servers in data centers located around the world. [30] In addition to providing security and scalability, these data centers offer load balancing, redundant (n+1) equipment, no single point of failure, and multiple network connections

to various network providers. [30] PlaceWare has redundancy built into its infrastructure, an infrastructure that is also extremely scalable.

Redundant equipment and spares accommodate peak load capacity issues. Several ways exist to minimize adverse effects in the event that a presenter's computer or Internet connection crashes.. Multiple presenters can simultaneously conduct a meeting, so if one presenter experiences a computer or Internet connection problem, other presenters can continue running the meeting. Presenters can upload their content to the PlaceWare service, where it remains in the password-protected meeting area until deleted and can be accessed from any computer connection. So if a presenter's computer crashes, any other computer with an Internet connection can be used to drive the meeting instead. [30]

The PlaceWare solution is extremely scalable. With Conference Center 2000, it can scale to over 5000 concurrent meetings with over 100,000 concurrent participants system-wide—with up to 2500 audience members in any single meeting, participating from anywhere in the world. [30] Scalability extends to dial-up users. PlaceWare's redundant network infrastructure design has led to its leadership in dial-up reliability. [30]

WebEx – Like PlaceWare, WebEx's network features include globally distributed hubs. WebEx continuously expands its international network of communications hubs to ensure scalability, performance, and global reach. Additionally, Network load balancing occurs 24/7. The WebEx MediaTone Network can be described as a distributed architecture that prevents any single point of failure and allows the network to efficiently manage the heavy traffic during business hours around the world. [25]

WebEx supports current and future industry standards such as: XML, H.323, T.120, and IMPP.

- **XML** - WebEx is leading the way in defining XML-based interactive e-commerce and e-marketplace standards. This standard

provides high level APIs for access to underlying WebEx Multimedia Switching Platform functionality. [31]

- **H.323** - Designed to foster interoperability between IP-based A/V solutions, H.323, depicted in Figure 3, is another standard for audio and video communications established by the ITU. WebEx technology supports this important standard which defines a number of functions critical to audio and video communications and fosters compatibility between solutions. [31]

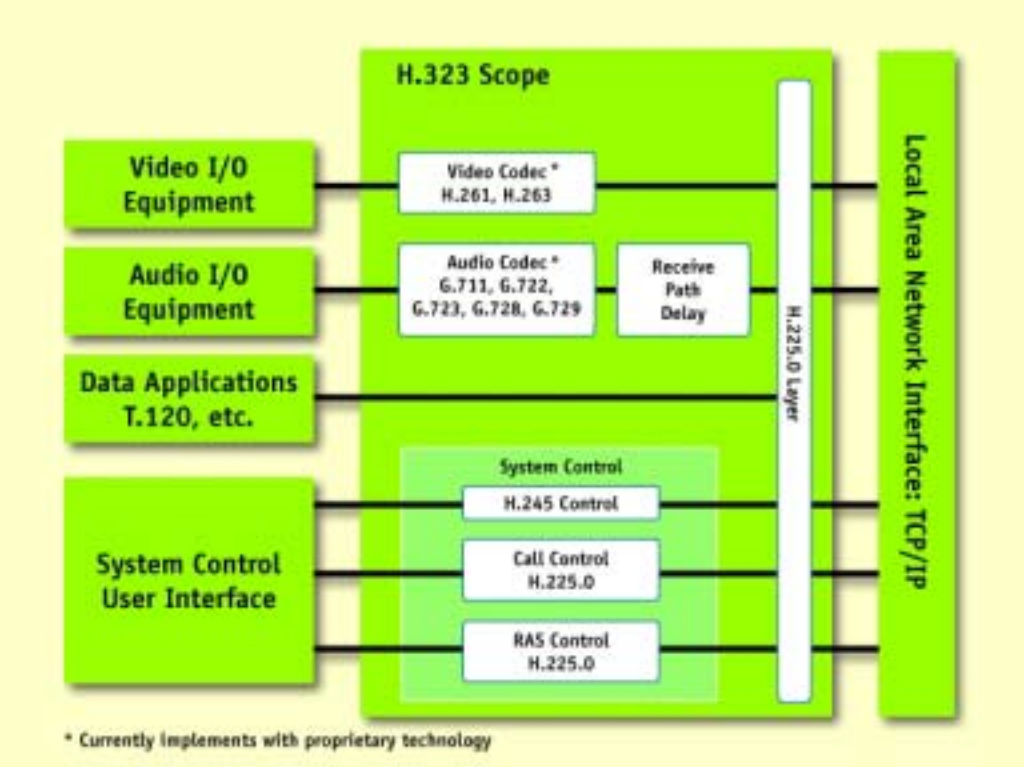


Figure 18. H.323 Scope (from [31])

- **T.120** - A suite of networking protocol standards for real-time multi-point data communications, T.120 is another critical specification established by the ITU and supported by WebEx. In addition to interoperability, the T.120 standard was established to ensure a long list of benefits that include data integrity, network

transparency, platform independence, network independence, and scalability. Figure 4 depicts several layers that comprise the T.120 standard.

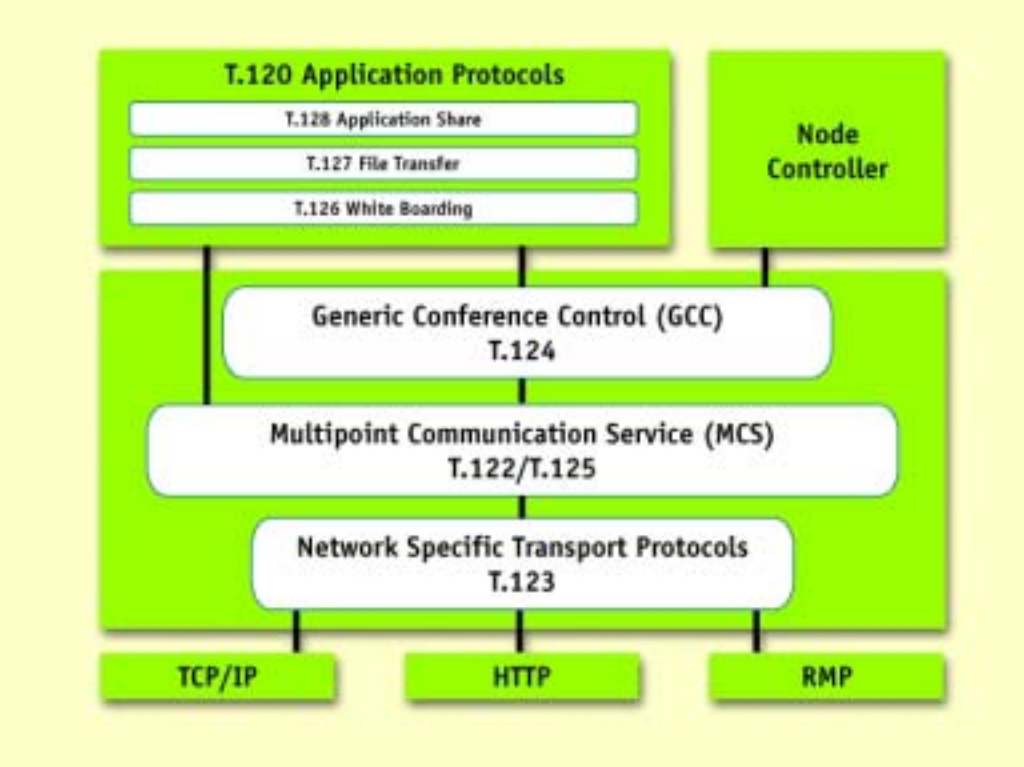


Figure 19. T.120 Application Protocols (from [31])

- **IMPP** (Instant messaging/presence protocol) - Many companies that are dedicated to forwarding Web-based communications are working together to develop the instant messaging/presence protocol (IMPP). Shortly, this standard will gain approval from the Internet Engineering Task Force. WebEx plans to support IMPP. [25]

Groove - Groove software's unique decentralized architecture provides an agile, secure and extensible collaboration infrastructure to support inter-agency decision-

making. The software, which is used by more than 40 government organizations, provides secure communication across unsecure networks, supports mobile users, is self-synchronizing and isn't highly vulnerable to attack, because like WebEx it doesn't have a single point of failure. [23] Users can deploy Groove Workspace (and new tools and toolsets) quickly, without the intervention of an IS/IT department, ISP or Web-hosting service, or reliance on third party or internal servers. Groove requires very little setup time. End users simply download the Groove Desktop environment and install it on their computer. Additionally, there aren't maintenance or system administration requirements. [33]. Groove also utilizes two-way synchronization, Visual Studio.Net, and servers that include Enterprise Management and Enterprise Integration.

Groove utilizes two-way synchronization between a Groove shared space and a Microsoft SharePoint Team Services (STS) web site. This is accomplished by a separately licensed Groove toolset called the Groove Mobile Workspace for SharePoint, this bit of integration will appear more seamless to the STS user than it will to the Groove user. That is, the Groove user will not find the expected STS 'Response Button'. More so, the Groove developer's GWS (Groove Web Services) won't find STS discussion data mapped to an accessible Groove discussion. [34] The STS file repository is, however, mapped to a standard Groove file repository, and STS lists (events, tasks) map to Groove forms. STS is not very clever about tracking unread items, for example, except by means of the overkill solution of e-mail notification. [34] Groove's change notification is more subtle and more effective.

Groove has a tool kit for Visual Studio.Net, and advanced Groove users familiar with the internal architecture are able to develop their own Groove space tools. In addition, the Groove Workspace supports elegant SOAP API for integration into the Groove environment; however, as of now, these API's are incomplete and pending further support in a later release for instant messaging and forms data. [34] During Security Evaluation Laboratory (SEL), it was found that adding relay servers improved communication availability among occasionally connected users and through all network topologies. [39]

The Groove Enterprise Management Server provides IT managers with centralized services for administering the deployment and use of Groove within an enterprise, agency or department. These services include usage management and reporting, and device policy management. [39] With the Groove Enterprise Integration Server, authorized members of Groove shared spaces can securely access, share and work with the external data residing in an organization's centralized, server-based, business systems (e.g., transactions records management, knowledge management, CRM, PRM). The Groove Enterprise Integration Server includes IT administration features and a rich set of APIs that allow enterprise developers to build integration solutions. [39] Integration is done with agent programs called “bots.” The Enterprise Integration Server provides several means to ease bot development. Developers can define deployable scripts to configure a bot run-time environment. Classes are provided to help with functions common to most bots. Also, bots can be written with common developer tools and languages, such as Visual Basic, JavaScript, VBScript and C++. [39]

ADLS (Advanced Distributed Learning Systems) - Fully operational ADLSs require a robust data and video network infrastructure between the decentralized databases and repositories for digital courseware and geographically-dispersed or mobile learners. Regarding military application of ADLS, network infrastructures must be interoperable between force components, echelons, delivery platforms, and user terminals. [18] The network infrastructure must be compliant with the Department’s Joint Technical Architecture (JTA), should be transparent to courseware developers, administrators, users, and managers, and should build on the existing infrastructure. [18] Integrated adaptive networks, interoperable platforms, databases, and related software must be developed and configured to ensure transparent access and the use of appropriate and authorized courseware. ADLS management and support sub-systems will be decentralized and, because they will be interoperable, will ensure continuous global access to registration, testing, record keeping, business-process, and expert-help functions. [18]

3. Secure Collaboration

Authenticating the identity of an end user is a key factor in effective collaboration. Additionally, data transmitted during the collaboration must be received with a level of assurance that it was not subjected to tampereing. In order for an organization to successfully employ a collaborative solution, security implications and concerns must be addressed in the framework of industry standards.

a. Implications

In the area of network security, one cannot ignore the implications associated with using collaborative tools. Implications such as: identity theft resulting from weak authentication procedures, information altering due to insufficient data integrity measures, and denial of service types of attack resulting from weak protocol implementation. These types of security concerns have largely hampered the growth of collaborative environments outside the local intranet. Seeing the future of sharing information through the use of collaborative environments, development companies are concentrating on security concerns associated with collaborative solutions. Some security measures, such as firewalls and encryption/decryption schemes, can greatly affect the robustness and/or the efficiency of the application. For example, firewall policies/rules can adversely effect communication between nodes, encryption/decryption schemes can effect transmission times, and key distribution techniques could negatively impact application ubiquity.

b. Security Concerns

Authenticity of the users and information integrity are the primary security concerns that surround the use of multicast protocols and associated firewalls in collaborative environments. The effects of firewalls on multicast protocols and applications can be profound. For the security conscious organization, a collaborative

network environment presents unique challenges. Organizations, both large and small, commonly have network security directives that address security issues associated with collaborative environments. Understandably, large organizations, such as the Department of Defense, are required to maintain networks that are hardened against malicious intent. Firewalls with strict security policies coupled with Intrusion Detection hardware and/or software make for a network's initial line of defense. When you add in information retention and auditing requirements, the organization is faced with even more challenges. To enable real-time communication, these organizations must implement complete management control over identity and authentication services and message logging. [8] Unfortunately, increased network hardening normally results in less effective collaboration. Collaboration robustness is inversely proportional to the degree of security an organization must employ to meet its mission. For example, assume a low bandwidth user is forced to participate in an encryption/decryption scheme that is computationally expensive (e.g. encrypting/decrypting large amounts of streamed media). Depending on the computational strength of the device (e.g. desktop, laptop, PDA) being used and the encryption/decryption intervals, this same user is not only operating in a low bandwidth environment; but also, is faced with potentially being unable (or has limited ability) to participate in a 'secure' streaming media-based collaborative environment. A balance between robust collaboration and a secure network must be achieved.

c. Security Standards

Federal Information Processing Standard 140-1 (FIPS 140-1) and its successor FIPS 140-2 are US Government standards that provide a benchmark for implementing cryptographic software. [42] They specify best practices for implementing encryption algorithms, handling key material and data buffers, and working with the operating system. An evaluation process that is administered by the National Institute of Standards and Technology's (NIST) Cryptographic Module Validation (CMV) Program [41] allows encryption product vendors to demonstrate the extent to which they comply with the standards, and thus the trustworthiness of their implementations. Some US Government agencies purchase only FIPS 140-1 or FIPS 140-2 evaluated encryption

products [40]. However, the security community-at-large values products that have completed this evaluation; completion carries with it the weight of a credible independent third party evaluation. [42]

d. Security in Application

Microsoft Office Live Meeting 2003 – Microsoft Office Live Meeting 2003's collaborative solution PlaceWare protects a company's sensitive information using a combination of advanced computer hardware and software technology, as well as security policies and procedures, which ensure that no unauthorized visitors can view presentation content or participate in private meetings. In addition, PlaceWare gives meeting leaders the flexibility to define the appropriate level of security required for the type of meeting being conducted. [30] Other security areas include: built-in security features, layered data security, and encrypted transmission security.

PlaceWare's built-in security features include: meeting passwords, access control lists with username/password pairs and open meetings. PlaceWare offers a choice of three authentication methods to control meeting access, Access Control Lists, Meeting Keys, and Open Meetings. [30]

PlaceWare protects any content you upload into their system with nine layers of security—providing both physical and logical protection of presentation content from unauthorized access [30]. The PlaceWare data center is protected by state of the art technology including motion sensors, video surveillance cameras, biometric controlled access, and security breach alarms. [30]

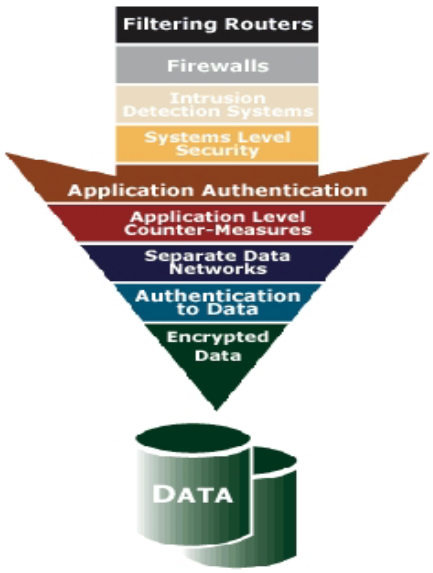


Figure 20. PlaceWare's Layers of Data Protection (from [30])

PlaceWare's services are protected by encryption of data to prevent "snooping" of sensitive meeting information. PlaceWare offers optional SSL encryption to protect all data as it is transmitted over the public Internet. PlaceWare's encryption consists of industry standard 128-bit RC4 SSL encryption. [30]

With respect to Microsoft Office Live Meeting 2003's SharePoint Portal Server 2003, a random port number is generated for the SharePoint Portal Server central administration pages. When there are multiple servers in a server farm, the port numbers for the central administration pages are different on each server, making remote administration cumbersome because the administrator must know the port number for the page for each server. To simplify remote administration, the option of eliminating random port number generation is available. This is accomplished by changing the port number to be consistent on all servers on the server farm. This allows the URL to be typed for the central administration pages without going through the Site Settings page for each server. From a security perspective, not using random port number generation makes the network more susceptible to malicious intent. With this option selected, if the port number of one server is known, all of the servers in the server farm are accessible.

The tradeoff between security and the convenience of simplifying remote administration is a continuous consideration. [28]

Groove – Groove has very extensive security built-in that is active by default. SharePoint offers some security features, but none as deep as those that are always-on within Groove. Groove implemented a unique solution to cross-boundary trust about which people working on projects such as Microsoft's future "TrustBridge" initiative for federated trust have only theorized. Ray Ozzie commented, "While most people are talking about trust at the enterprise level, and big-iron solutions to federation of trust, Groove has managed to figure out a way to implement 'complacency-immune' security at the data confidentiality level as well as at the authentication/trust level, even in cases where administrators aren't able or willing to federate their (potentially incompatible) infrastructures." [35] Other areas of Groove security include data encryption, Enterprise Management and Integration Servers, and government certifications.

All data in Groove Workspace is automatically encrypted, both on hard-disk and while moving over the network. Peer-based authentication ensures confidentiality. End-to-end encryption ensures integrity of content and activity, even for users who don't care about security. Shared spaces are private, only invited members can see or create content. [33] Groove Workspace enables real-time, inter-enterprise interaction by automatically and transparently crossing firewalls. Users never need to go through special steps to set up shared spaces with third-parties such as customers, partners or suppliers. [33] Groove's strong software security, currently under NIST review, can transit organizational boundaries transparently. Dr. Bordetsky states in [21], "The overall combination of encryption and data sharing features provides a good solution". Here, Groove designed its product to operate in a decentralized, peer-to-peer model over the Internet and work seamlessly across different firewall configurations. It also doesn't circumvent firewalls or otherwise introduce new security risks because it is fundamentally an XML Web services-based offering. Whereas, SharePoint in not as

flexible across firewalls. For instance, it requires a VPN connection for some usage scenarios. [35]

Figure 21 provides an overview of Grooves Security Services. All Groove communication uses public-key infrastructure, X.509, which is an internet standard for ITU PKI standards. Groove's security policy can be enforced at the company level with an administrator certification or at a person-to-person level with manual certification. Manual certification occurs by using digital fingerprints. Additionally, all 'official' component downloads are digitally signed by Groove. Users are given a choice to trust unofficial component downloads.

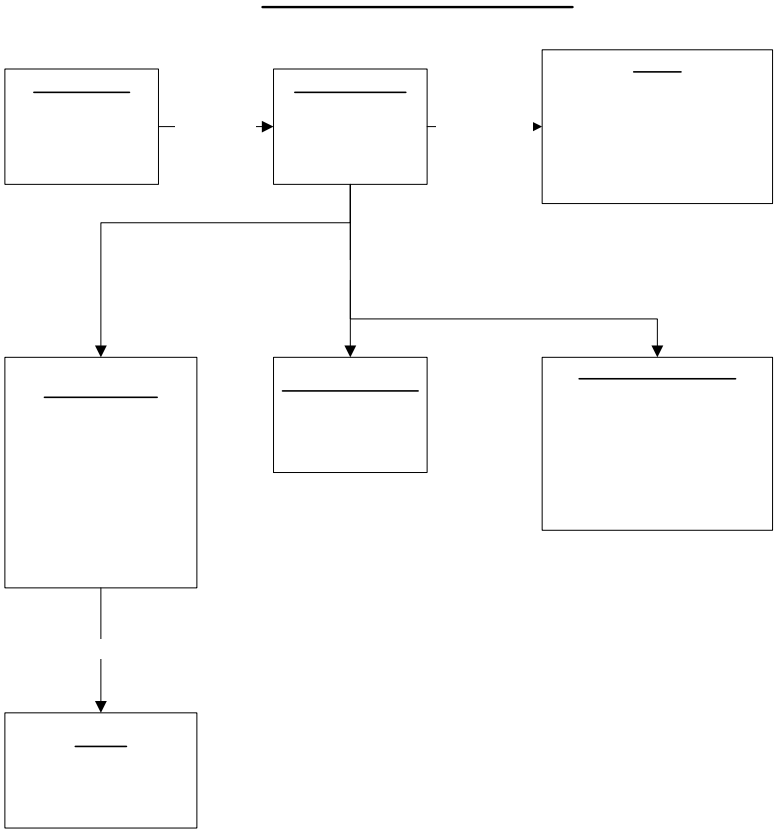


Figure 21. Groove Security Services

If the Groove Enterprise Management Server is employed, the authentication menu will inform you if a contact is part of your domain. If not, then a process of direct authentication occurs. Steps include: 1) contact person outside of

Groove, such as by phone, 2) ask them to tell you their digital fingerprint, 3) compare it to the digital fingerprint displayed in the authentication menu, 4) If the fingerprints match, then process concludes with the user checking the “Authentication As” box in the Authenticate menu. Once authenticated, the digital fingerprint will be used to verify data integrity of future correspondence with the owner of the fingerprint and the authenticated individual can now participate in shared spaces. Figure 22 depicts the timeline process of inviting someone into a shared space.

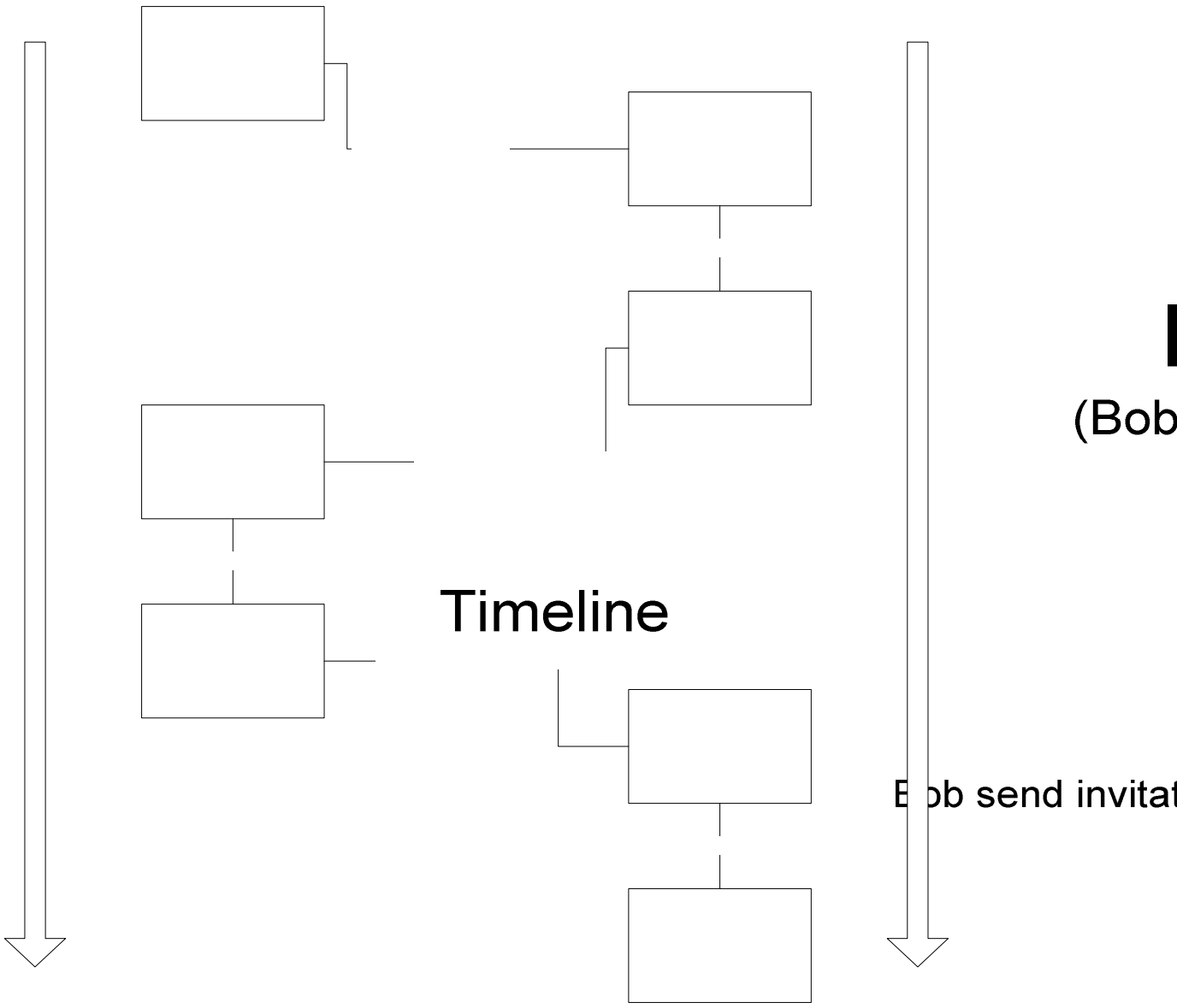


Figure 22. Inviting People to Shared Spaces

For applications that require integration with non-Groove systems and data, the Enterprise Integration Server automates secure, bi-directional information flow. The Enterprise Management Server provides organized control and administration for all users and servers. [39] “The Groove Enterprise Relay Server eases inter-enterprise,

agency and department enterprise communications across security domains by traversing through firewalls, proxy, and NAT devices. The Enterprise Relay Server behaves as an HTTP proxy, automatically 'wrapping' messages within HTTP, so they can pass easily through the firewall. This process, called 'HTTP tunneling,' allows users to transparently establish and conduct purposeful interaction without the intervention or assistance of network administrators. This relieves the IT manager of the burden of setting up and maintaining special purpose, secure extranets for cross-firewall domain business interaction." [39]

Additionally, Groove software is undergoing evaluation to certify that it meets claims for cryptographic support as defined by the Common Criteria for Evaluation Assurance Level 2 augmented (EAL2+). This certification is granted by the U.S. Government National Institute of Standards and Technology (NIST) through the National Information Assurance Partnership (NIAP). Currently, the cryptographic module used by Groove software, Crypto++, meets the newest Federal Information Processing Standards (FIPS) for FIPS 140-2 level 1-approved security requirements for cryptographic modules. [39] This certification approves the findings of Entrust Cygnacom, a NIST-accredited Cryptographic Modules Testing (CMT) laboratory that evaluated Crypto++ and submitted its recommendation for approval to NIST. [33] With this certification, grooveNETWORKS is among the first companies in the commercial sector committed to FIPS/NIST certification. For companies considering collaboration solutions, this commitment protects the privacy and integrity of an organization's communications, data, and intellectual capital. [37]

4. Efficient Collaboration

As bandwidth availability increases, so does the desire to implement more robust (i.e. higher bandwidth) collaborative solutions. Many collaborative tools have the highest bandwidth requirements. It's important to recognize that collaborative solutions are not hampered by bandwidth, but that available bandwidth is what hampers ubiquitous distribution of collaborative solutions. One of the most bandwidth intensive collaborative

tools falls into the streaming multimedia category. New protocols and technologies are being developed to address efficient network distribution of streaming multimedia. When streaming media in a collaborative environment, the various protocols utilized to deliver the media will determine the level of efficiency at which the collaborative tool operates. Security and associated firewalls are severe efficiency blockers if the collaborative solution does not compliment the network architecture. Both, multicast protocols/applications and firewall interaction pose serious network efficiency concerns. Prior to choosing a collaborative solution, a comparison of each available solution (preferably multi-cast based) should be accomplished. Due to the architecture of a multicast-based solution, it provides the greatest network efficiency when collaborating outside of a one-to-one environment (i.e. it's more efficient with one-to-many or many-to-many type environments).

a. High Bandwidth

The advent of gigabit and Fast Ethernets, have greatly increased the potential of collaborative environments. The more robust a collaborative solution is, the higher are its bandwidth requirements. Current multicast limitations found in network architectures (e.g. non-multicast routers), non-multicast supporting firewalls, and authentication/information integrity encryption/decryption schemes will hamper the growth of multicast applications in the near future. However, as these limitations are addressed, more efficient and secure multicast applications are developed, and larger data pipelines become available, the implementation of collaborative environments will definitely follow.

b. Benefits of Efficient Collaboration

When choosing a collaborative solution, network efficiency should be a valid concern. The benefits of streaming media with a multicast-based collaborative tool is quickly realized when multiple streams are required simultaneously.

All organizations are not created equal. An organization must first determine what collaborative solutions will 'best fit' their organization. Collaborative solutions vary in efficiency, security and robustness. If an organization has low bandwidth users or high security level requirements, then efficient encryption/decryption schemes and data transmission will be of primary concern. In contrast, if an organization thrives on 'face time' (i.e. distance learning, command and control, video conferencing, etc), then a more robust feature such as video and audio streaming will be part of the organizations tool set and depending on their level of security, efficient encryption/decryption schemes may also be necessary.

c. Drawbacks of Multicast-based Collaboration

Identifying multicast-based collaboration challenges will help to ascertain the feasibility of implementing a collaborative solution for an organization. If an organization's network does not support multicast, the initial expense of upgrading firewalls, switches, and/or routers must be taken into consideration. Additionally, depending on network architecture, configuring the network to efficiently handle multicast traffic can be challenging and labor intensive. If the multicast network is not correctly configured, problems such as unintentional flooding of the network with multicast packets can occur.

d. Efficiency in Application

Groove implements a scheme that is sensitive to bandwidth optimization. When one member of a shared space makes a change to a large document, Groove Workspace sends only the changes, optimizing limited network bandwidth. New Files-on-Demand features in Groove Workspace 2.5 allow users working over a slow connection to receive only those files that they need at the moment, further optimizing bandwidth. Also, Groove Enterprise Relay Server improves the efficiency of communication over low-bandwidth Internet connections. In cases where a Groove

Workspace user is connected through a slow communication link and needs to transmit large amounts of data to several users, Groove Workspace will send a single copy to the relay server, which will in turn, send a copy of the data to each user within the shared space. [39]

C. COMPARISON SUMMARY

The act of comparing collaborative solutions is difficult because of the simple fact that collaboration is evolutionary; hence, it can not be held to a distinct point in time. In the recent past, compression technology has improved, design upgrades have cut costs, and a new generation of videoconferencing systems designed to work over IP networks, as well as ISDN connections, is gaining a foothold in corporations.

This section compared several collaborative solutions which included many available collaborative tools/features, architecture, security, and efficiency issues. The specific comparison areas included real-world applications/examples of Microsoft Office Live Meeting 2003, WebEx, and/or Groove. Figure 23 below is a collective presentation of the collaborative solutions compared in this thesis. Network type, organization size, scalability varies among the solutions compared. Each of the solutions has access controls and utilizes standard Encryption techniques. With respect to transiting firewall, the Groove solution is the most versatile due to its encapsulation technique. Groove only transmits deltas (i.e. changes) to shared information, thus enjoys greater bandwidth efficiency when transmitting data. SharePoint and WebEx are data, voice, and video capable and both offer multicast support, where Groove only offers a voice feature, a major shortcoming for a collaborative solution. Multicast capability is an important factor when considering a collaborative solution. If an organization conducts distant learning and/or video conferencing in a one-to-many or a many-to-many configuration, the multicast-based features will ensure the greatest network performance.

Collaborative Solutions Summary

	Network Type (Centralized Decentralized Hybrid)	Organization Size	Access Controls	Firewall Transparency	Standard Encryption Techniques	Bandwidth Efficient	Data, Voice, and Video Capable	Multicast Support	Scalable
SharePoint	Centralized with Hybrid capabilities	Large and Small	Yes	No	Yes	No	Yes	Yes	High
WebEx	Decentralized	Large and Small	Yes	No	Yes	No	Yes	Yes	High
Groove	Decentralized with Hybrid capabilities	Small and Medium	Yes	Yes	Yes	Yes	No (Data and Audio only)	No	Low

Figure 23. Summary of Collaborative Solutions

The purpose of this section was not to select the best possible solution through an unrealistic, exhaustive analysis of each available collaborative tool, but to impart upon the reader areas of concentration that will assist in selecting a collaborative tool that fits a particular organization. Also and more specifically, the section's purpose was to point out the availability of numerous collaborative solutions, some of which were then provided as examples to further assist the reader's understanding of collaborative network architectures, security, and efficiency concerns.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION AND RECOMMENDATIONS

This thesis informed the reader why collaborative environments are important in today's online productivity. A comprehensive background in collaborative environments was provided and the thesis described how collaborative environments are employed in the Department of Defense and industry. In addition, the thesis presented a comparison of collaborative solutions with a focus on security. As a secondary focus, the thesis also presented the effects of network security on multicast protocols. In conclusion the following items are presented: collaborative concerns and differences, the Groove and Microsoft relationship, Advanced Distributed Learning in DoD, and a recommendation for collaborative solutions to be utilized by NPS/DoD type networks is provided next.

A. COLLABORATIVE CONCERNS AND DIFFERENCES

The predominate concern of network security leads today's enterprise users to communicate via VPNs (virtual private networks) and dedicated private IP networks. It is believed the guaranteed levels of quality-of-service experienced while using VPNs and private IP networks cannot be offered by the public Internet. It is also believed while some quality-of-service standards are in place today; they can be described as "fluid and incomplete." [46] The security and efficiency chapters contrast with the previous statement. These chapters depict and support the fact that the public Internet is capable of providing guaranteed levels of quality-of-service. Collaborative environments have moved beyond the "fluid and incomplete" stage and are able to provide quality-of-service guarantees while simultaneously addressing organizational security concerns.

Another predominate concern is recognizing that until maturing protocols, such as the Internet Engineering Task Force's evolving Session Initiation Protocol (SIP), gain a stronger foothold, standard videoconferencing interfaces, such as the ITU's H.323 [46], will continue to experience integration problems when adding audio calls from voice-over-IP telephony systems, which use SIP or proprietary protocols, to establish a videoconferencing session. Another challenge end users are faced with is the necessity of

knowing the destination IP address or phone extension to establish a session. Some products allow the creation of an address book, but most can't access information already stored in an Active Directory or other enterprise directory infrastructure. [46] Disconnects such as these have prevented full implementation of collaborative solutions; however, despite its limitations, collaborative functions such as IP videoconferencing can pay off in organizations that require more than 30 hours of videoconferencing per month. [46] A cost/benefit analysis, taking an organization's current network architecture and prospective collaborative solution into consideration, would be necessary in determining if a collaborative solution will payoff.

B. WORKING TOGETHER, GROOVE AND MICROSOFT

Prior to making a decision on which collaborative solution to implement, it's important for Microsoft oriented organizations to understand the Groove/Microsoft relationship. After its October, 2001, investment in and partnership with Groove, Microsoft positioned Groove as a complementary product for customers who sought to easily collaborate across firewalls or have off-line capabilities for documents and SharePoint (SharePoint Team Services, at that time) sites. [35] More recently, with the introduction of SharePoint products and technologies for 2003, Microsoft goes further with document-level off-line and re-synchronization support. But Microsoft still works with Groove for customers needing collaboration support across firewalls and for workspace-level synchronization. [35] The new SharePoint offerings also have prerequisites - for instance, Windows SharePoint Services will only run as part of Windows Server 2003 - that will lead some organizations to consider Groove and its support for previous releases of Windows and Office.

Conceptually, Microsoft Office is still a document-centric system, enhanced with real-time services for presence awareness and real-time communication. Conceptually, Groove focuses more on verbs than nouns; it assumes a decentralized shared workspace context and delivers collaboration and powerful off-line/re-synchronization capabilities by asynchronously disseminating actions (verbs) within the shared context instead of

replicating documents (nouns). This results in a different form-follows-function fit, despite some overlap and synergy. It's certainly not a right-or-wrong or either-or scenario. As previously noted, Groove and SharePoint were designed to address different customer needs, and their architectural differences are more complementary than competitive. [35]

Small or ad-hoc workgroups need informal, end-user driven tools to work together on shared content. Workgroups need to share information easily and effortlessly, both internally and cross-enterprise, without requiring IT support and intervention. [35] Together, a combined SharePoint and Groove Workspace solution provide users with easy to use, end-user collaboration tools with the unique benefits of offline access to portal content, automatic synchronization, and secure real-time collaboration across network boundaries.

Going forward, and especially when Microsoft ships the Longhorn versions of Windows and Office, the Microsoft/Groove relationship will continue to evolve. Longhorn, for example, will include a new Windows File System that natively supports a broader range of replication services, although it probably won't be deployed broadly within organizations until the 2005 to 2006 time frame. [35] The simple fact that Microsoft is focused on the future of collaborative environments should be weighed while considering a collaborative solution. It can be argued that the emerging Window's File System will cause Groove will fade away in 2 or 3 years. This author does not believe this will be the case, as the Groove team has established a unique track record for complementing Microsoft products and technologies, and the team also has unprecedented experience in collaboration tools, including PLATO, Notes, and Groove. [35] Its unique relationship with Microsoft also bodes well for its future.

C. DOD AND THE ADVANCED DISTANT LEARNING INITIATIVE

A significant Department of Defense initiative, Advanced Distributed Learning System (ADL), proposes to leverage commercial off-the-shelf (COTS) software and successful public, private, academic, and industrial initiatives for the benefit of the

Department. Department of Defense organizations and doctrines for learning will co-evolve along with a robust DoD ADL to meet the requirements of our future military forces. [18] However, prior to implementing an effective advanced distributed learning system, DoD ascertains the necessity of five elements [18] that need to develop in order to successfully implement the ADLS: 1) common industry standards, 2) interoperable tools and content, 3) robust and dynamic network infrastructure for distribution, 4) supporting resources, and 5) cultural change at all levels of command that recognize that learning is an official requirement of the duty day. Each of these five elements is congruent and applicable to industry which in turn is also driving the development of collaborative environments and advanced distributed learning systems.

The nature of the advanced distributed learning strategy recognizes the existence of traditional impediments and barriers to change. Independent systems, proprietary processes, and lack of interoperability can delay implementation and reduce expected returns on investment. One of the biggest issues in the cost-benefit analysis of advanced distributed learning is that, under current accounting systems, organizations making the investment in learning often are not the organizations which are reaping the benefits. Unless the Department removes such structural counter-incentives, they will be certain to impede progress. [18] The existence of these counter-incentives fuels the slovenliness of DoD technical adaptation to emerging technologies.

In short, architecture will be expected to support a wide range of interactive multimedia instruction including real-time, full-motion video and audio, as well as, document sharing and collaborative communications with instructors, experts, and other learners. This also means there will be a variety of interactive multimedia instruction format types and some of them will be bandwidth intensive. Therefore, the architecture will have to account for bandwidth implications, the role of hybrid distributive media formats, and emerging media technologies such as desktop videoconferencing, streaming media, and voice telephonic applications.

D. GROOVE, NPS AND MULTICAST RECOMMENDATIONS

Without a doubt, the Groove solution provides the necessary bridge towards effective collaboration not only in distant learning, but also in distributed collaborative research among several institutions/organizations. As far as the near future is concerned, further implementation of Groove at NPS will facilitate collaborative research. Collaboration among distributed nodes at NPS and across the Internet makes Groove a smart choice as a collaborative solution that complements NPS's current network architecture. The Naval Postgraduate School's primary distant learning tool, Blackboard, lacks in the areas in which Groove excels. Dr. Bordetsky sums it up the best, he emphasizes in [21] that the unique level of "shared awareness" offered by Groove is a key benefit that helps dispersed teams self-organize around contextual information. Furthermore, Groove allows you to monitor workflow at the application level, something people need desperately when they transfer collaborative work out of the physical space to the virtual space. A second major benefit Groove provides is a very well-refined balance between asynchronous and synchronous collaboration capabilities.

Unfortunately, Groove does not utilize multicast-based tools, nor does it function well in low bandwidth environments. However, the design of the Groove desktop environment is centered on small collaborative networks that desire to securely share information among widely dispersed end users, a feature that is highly desirable among research-based institutions. Considering Groove's recent certifications and features presented in Chapter 5, it is strongly recommended that NPS further expand the Groove desktop environment. The expansion should include all professors, research associates, students and research sponsors that collaborate toward common research goals.

NPS will be implementing Cisco's PIX 6.2 firewall in the Spring of 2004. As presented in Chapter 4, this firewall provides excellent multicast support, thus it makes sense, and is recommended, for NPS to invest in a large scale (i.e. enterprise level) multicast-capable collaborative solution. Both PlaceWare and WebEx solutions serve this purpose. Either solution will enable NPS to better utilize the new firewall's increased multicast bandwidth capabilities to communicate and collaborate with other DoD and academic institutions. With the ability to stream real-time media, NPS's general student body would be able to simultaneously subscribe to the same broadcasted information (e.g. Student Guest Lecture, General Military Training, etc). With an

enterprise level collaborative solution, NPS and other DoD organizations would be able to take advantage of the many benefits depicted in Chapter 3 (Collaborative Environments in DoD and Industry).

E. CLOSING STATEMENT

It's been said, "There are two reasons people are seeking out collaborative tools today: First, everyone is more mobile, and business is more global. Second, there is much more partnering going on, both inside organizations, and between organizations". [1] The reader must understand there exist possibilities for distant and/or distributed learning solutions associated with the network communication infrastructure for delivery, bandwidth considerations, warehousing, and use of commercial off the shelf (COTS) software. However, it is not clear that a total COTS solution is attainable today. While comparing solutions, it's important to select a solution that is flexible enough to complement an organization's network infrastructure and security requirements, while at the same time the solution should be robust enough to take advantage of what current technology is offering.

Regarding security and firewall issues related to multicast transmissions in collaborative environments, it should be recognized that multicast packet storms (inbound or outbound) are not currently handled by firewalls. In the event of a multicast packet storm, the routers and/or switches will be forced to handle such storms. The continued ubiquitous deployment of multicast-based applications will increase the potential and frequency of multicast packet storms which can severely impact network performance and security. Future firewalls will evolve and be able to handle multicast packet storms lending greater efficiency and security to associated subnets.

F. FUTURE WORK

Related areas of research could possibly include: solutions to handle multicast packet storm effects on network security and efficiency; solutions to handle multicast

packet storms; MAC level multicast filtering at the firewall to increase network efficiency; multicast vs. unicast and/or broadcast collaborative/ADL solutions; migrating from unicast-based collaborative environments to multicast-based collaborative/ADL environments; and migrating DoD's legacy collaborative/ADL solutions to secure enterprise and/or web-based collaborative solutions.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

[1] Ore, Joel. "Groove: Irresistible Collaboration." [http://www.extranetnews.com/2003%20issues/EXTRANETNEWSWeekof24Feb2003.htm]. 24 February 2003

[2] Ozzie, Ray. "Perspective: A mosaic of new opportunities." [http://news.com.com/2010-1071-997725.html]. 20 June 2003

[3] Firewall.cx. "Introduction to Multicast." [http://www.firewall.cx/index.php?c=multicast-intro]. 18 August 2003

[4] Firewall.cx. "Media Access Control: MAC Addresses." [http://www.firewall.cx/mac_addresses.php]. 18 August 2003

[5] Firewall.cx. "Introduction to Firewalls" [http://www.firewall.cx/index.php?c=firewall]. 18 August 2003

[6] Firewall.cx. "Firewall Topologies"[http://www.firewall.cx/index.php?c=firewall_topologies]. 18 August 2003

[7] Naval Postgraduate School for INFOSEC Studies and Research. "Course notes for CS 3600." October 2001

[8] O'Kelly, Peter. "That Real-time Vision Thing" [http://www.mssmartsolutions.com/newsletterarticle/2003/07/vba2003/07/vba200307po_1/vba200307po_l.asp] 18 August 2003

[9] O'Kelly, Peter. "Evolutionary SharePoint" [http://www.mssmartsolutions.com/columns/2003/06/vba200306po_u/vba200306po_u.asp] 18 August 2003

[10] Winkler, Ramona. "Key Words and Definitions are 'Collaboration'" [complete reference with information found on laptop]

[11] Wan, Leong, and Thum. "Multicast Firewall for Intranet Multimedia Applications" [http://nrg.cs.usm.my/~tcwan/Papers/WEC99-Multicast-Firewall.pdf] 27 August 2003

[12] W. Stallings, "High-speed networks: TCP/IP and ATM design principles" Upper Saddle River, NJ: Prentice-Hall, 1998

[13] Microsoft Corp, "Understanding the H.323 Standard" [http://www.microsoft.com/windows/NetMeeting/Corp/reskit/Chapter11/default.asp#h323] 27 August 2003

[14] Wallner, Harder, Agee, "Key Management for Multicast: Issues and Architectures" Networking Working Group RFC 2627, June 1999

[15] Perrig, Canetti, dawnsong, tygar, "Efficient and Secure Source Authentication for Multicast" [http://www.ece.cmu.edu/~adrian/projects/tesla-ndss/index.html] 28 August 2003

[16] Perrig, Canetti, dawnsong, tygar, “Efficient Authentication and Signing of Multicast Streams over Lossy Channels” [http://www.ece.cmu.edu/~adrian/projects/stream/node1.html#SECTION00010000000000000000] 28 August 2003

[17] Finlayson, “IP Multicast and Firewalls” Networking Working Group RFC 2588, May 1999

[18] ODUSD, “Department of Defense Strategic Plan for Advanced Distributed Learning” Office of the Under Secretary of Defense for Personnel and Readiness, 30 April 1999

[19] CNET/CNO, “The Navy-Wide Distributed Learning Planning Strategy” Director of Naval Training (N7) Chief of Naval Operations, 04 December 1998

[20] Ore, Joel. “From our Readers” [http://www.extranetnews.com/2003%20issues/EXTRANETNEWSWeekof24Feb2003.htm]. 24 February 2003

[21] Groove, “Naval Postgraduate School” [http://www.groove.net/scripts/print.gtml?page=/customers/casestudies/education/naval.html] 20 August 2003

[22] Menke, Susan. “Shared Workspaces keep DoD docs in the know”, Government Computing News, Vol. 22 No. 4, 24 June 2003

[23] Groove, “Groove Workspace Software Obtains First Defense Collaboration Tool Suite V2.0 Interoperability Certification” [http://www.groove.net/about/press/releases/20030625dcts.html] 20 August 2003

[24] Smith, Colin. “Ingram Micro Uses WebEx Enterprise Edition to Facilitate Global Communications” [http://www.webex.com/pr/pr263.html] 05 September 2003

[25] Adler, Carolyn. “Computer Technology Services (CTS) Brings WebEx to Government Market” [http://www.webex.com/pr/pr266.html] 05 September 2003

[26] Microsoft “Microsoft Live Meeting a PlaceWare Service” [http://main.placeware.com/services/our_services.cfm] 05 September 2003

[27] Microsoft “Information Sharing and Collaboration for Growing Businesses” [http://www.microsoft.com/sharepoint/intranets/overview.asp] 10 September 2003

[28] Shroeder, Emily “Microsoft® Office SharePoint™ Portal Server 2003” Microsoft Corporation [http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itcommunity/chats/trans/Office/Off0424.asp] 10 September 2003

[29] Microsoft “Microsoft’s Real-time Collaboration Offerings Join Microsoft Office Family and Get “Live” [http://main.placeware.com/about_us/press_releases/press_release_dyn.cfm?ID=34] 10 September 2003

[30] Microsoft “Why PlaceWare Web Conferencing” [http://main.placeware.com/services/why_webconf.cfm] 10 September 2003

[31] WebX “WebX Standards” [http://www.webex.com/technology_standards.html#] 10 September 2003

[32] Groove “Groove Workspace Desktop Collaboration Software” [http://www.groove.net/products/workspace/] 10 September 2003

[33] Groove “Groove Workspace Benefits” [http://www.groove.net/products/workspace/benefits.html] 10 September 2003

[34] Udell, Jon “Uniting under Groove” InfoWorld // Test Center [http://www.infoworld.com/article/03/02/14/07groove_1.html?s=tc] 20 June 2003

[35] O’Kelly, Peter “Collaborating on Collaboration” SmartSolutionsNow [http://www.mssmartsolutions.com/newsletterarticle/2003/06/vba200306po_1/vba200306po_1.asp]

[36] grooveNETWORKS “Desktop Collaboration” [http://www.groove.net/products/workspace/certification.html] 11 September 2003

[37] grooveNETWORKS “Groove Government Certification” [http://www.groove.net/products/workspace/certification.html] 11 September 2003

[38] Udell, Asthagiri, Tuvell “Peer-to-Peer: Harnessing the Power of Disruptive Technologies” BYTE.com and grooveNETWORKS [http://www.groove.net/pdf/chapter18-security.pdf] 11 September 2003

[39] Entrust “Groove Networks: Groove Workspace and Servers, Version 2.0” [http://www.entrust.com/entrustcygnacom/labs/pfSEL0141A.htm] 11 September 2003

[40] Information Assurance Directorate “National Policy Regarding Evaluation of Commercial Products” [http://www.nsa.gov/isso/20020215memo.pdf] 11 September 2003

[41] NIST “Cryptographic Module Validation Program” [http://csrc.nist.gov/cryptval] 11 September 2003

[42] Microsoft “FIPS 140 Evaluation” [http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/issues/FIPSEval.asp] 11 September 2003

[43] Symantec “Symantec Enterprise Firewall 7.0” [http://enterprisesecurity.symantec.com/content/promotions.cfm?PDFID=40] 11 September 2003

[44] Hyman, Gretchen “Cisco Releases 6.2 Version of PIX Firewall Family” Internetnews.com [http://www.internetnews.com/xSP/article.php/974271] 11 September 2003

[45] Cisco “Cisco PIX Device Manager Release Notes Version 2.0(2)” [http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/relnotes/pdmrn202.htm#xtocid24] 11 September 2003

[46] Mitchell, Robert L. “Videoconferencing Gets IP Boost” Computerworld [http://computerworld.com/news/2003/story/0,11280,78884,00.html] 03 March 2003

[47] Joint Chiefs of Staff “Joint Operation Planning and Execution System” [http://www.dtic.mil/doctrine/jel/other_pubs/jopes.pdf] 21 September 2003

[48] 3 Com “SuperStack II Switch 2200 Operation Guide” [http://support.3com.com/infodeli/tools/switches/s_stack2/2200/ssopergd/obrdgex8.htm] 21 September 2003

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Geoffrey Xie, Professor
   Naval Postgraduate School

4. John Gibson, Research Associate
   Naval Postgraduate School

5. Alex Bordetsky, Professor
   Naval Postgraduate School

6. Lonna Sherwin, Computer Specialist
   Naval Postgraduate School

7. Tom Hazard, Deputy Director DLRC
   Naval Postgraduate School

8. Keith Felker
   Naval Postgraduate School